



Keeping Your Kids Safe Online - Do's and Don'ts

- Position the home computer in a way that children cannot easily conceal what they are viewing.
- Encourage children to only communicate with people whom they know and trust. Instruct them not to post any personal information or pictures that can identify schools attended, home addresses, friends, or family.
- Children with access to smartphones must keep in mind that photos taken by mobile devices will contain concealed location information.
- Utilize privacy and security settings available on web browsers to provide a basic filter for web content. Internet Explorer provides the most protection. Install supplementary protection software to maximize security through more granular protection and monitoring.
- Monitor your child's browser history and downloaded files for suspicious content, and prevent cookies from being stored on your computer. This will minimize the amount of personal information that can be exploited from your child's internet sessions.

Child Safety Online

Since 2012, minor's involvement with social networking services (SNS) has risen to 96%. It is reported that 69% of these users have received online communications from strangers. Common harmful interactions that children encounter online include cyber-bullying, coercion, pornography, drugs/alcohol, and violence. Dangers are not limited to content that a child receives, but also includes the information that a child makes public. Several web browser add-ons and software downloads are available to both prevent and/or monitor child activity.

Internet Explorer Browser Settings

To view child safety options, navigate to **Tools > Internet Options > Content**. Click **(1) Parental Controls** to customize individual user settings or click **Enable** under **(2) Content Advisor** to assign ratings to content categories.



Parental Controls

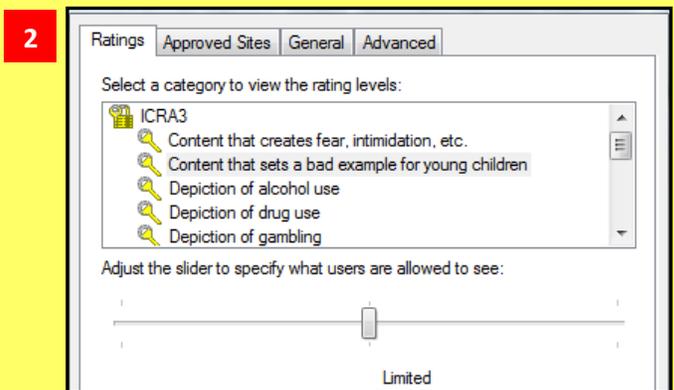
Adjust how your children can use the computer. Set personalized restrictions based on time, game ratings, and computer programs.

Passwords

Create a password for your child's account that only you and other adult supervisors know to ensure adult presence.

Time Restrictions

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



Content Advisor

Potentially harmful internet content is listed by category. Select a category and use the slider to set filters for individual content. Categories include:

- Content that creates fear, intimidation, etc.
- Content that sets a bad example for young children
- Depiction of alcohol use
- Depiction of drug use
- Depiction of gambling
- Depiction of tobacco use
- Depiction of weapon use, intimidation, etc.
- Incitement/ depiction of discrimination or harm
- Language
- Nudity
- Sexual material
- User-generated content
- Violence

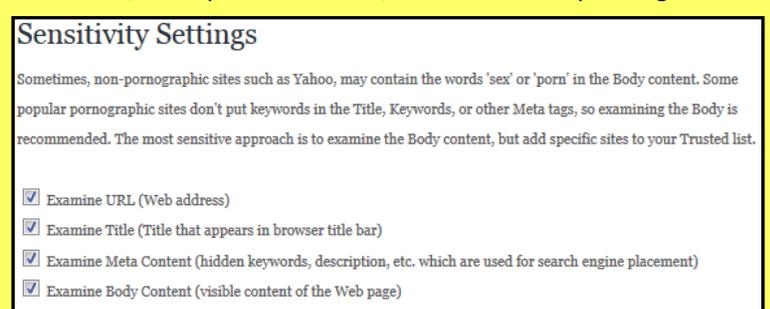
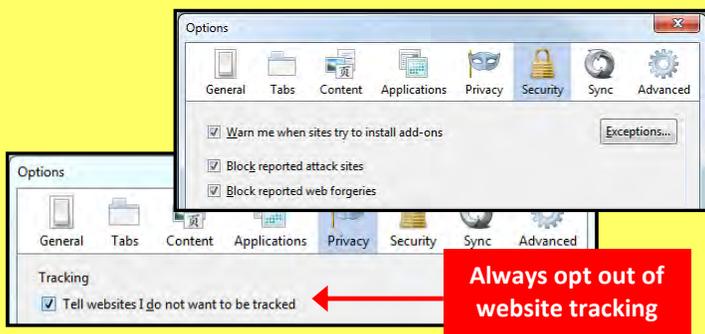
Set the slider to "None" or "Limited" for harmful content and set the slider to "Some" or "Unrestricted" for acceptable content.

When a category is selected, a description of each content category is listed under the slider, describing what your child will be able to view.

Firefox Browser Settings

Standard Firefox: Navigate **Settings > Privacy** to prevent web tracking and **Settings > Security** to block access to sites with malicious content.

Foxfilter for Firefox: To set parental controls, download the FoxFilter add-on. Once installed, navigate **Options > FoxFilter Settings** to allow select sites, set key words to block, and set sensitivity settings.





Keeping Your Kids Safe Online

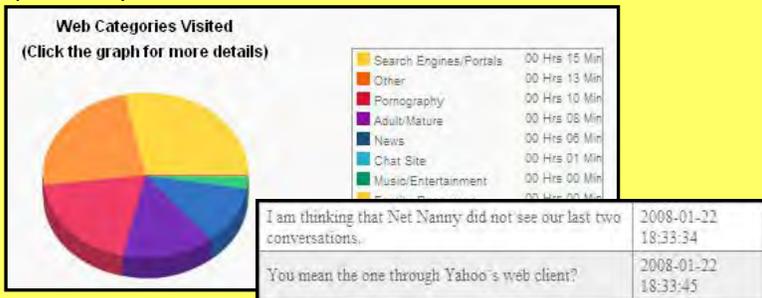
Child Safety 060513_1315

Software Protection

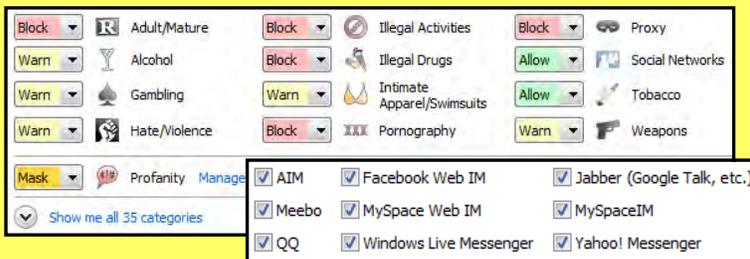
Service Capabilities	Software		
	Microsoft Family Safety	Net Nanny	EyeGuardian
Image Monitoring	Windows 8+	X	X
SNS Message Monitoring		X	X
Contacts Monitoring	Windows 8+	X	X
Block Sites Option	X	X	
Allow Sites Option	X	X	
Record User Activity	X	X	X
User Access Requests to Admin	X	X	
Time Restrictions	X	X	
Game Restrictions	X	X	
Paid Service		X	
Remote Access to Notifications	X	X	X
Lock Safe Search	Windows 8+	X	

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, 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.

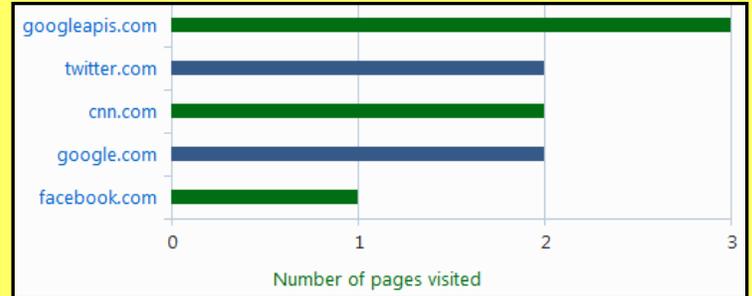


Overview

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

Microsoft Family Safety

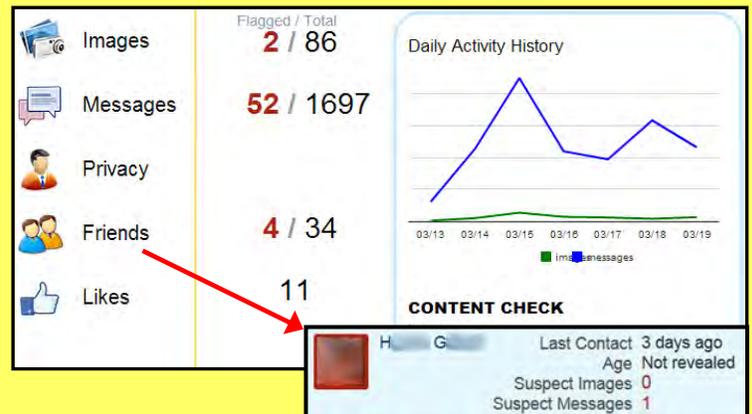
Download this free service from the Microsoft Windows website. The service provides basic content filters and reports of programs/websites accessed by each account.



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

EyeGuardian

Register online with this service to monitor your child's Facebook activity. This free service does not provide a way to prevent content from reaching your children but provides a way to monitor each interaction. The software graphically summarizes Facebook activity and automatically flags potentially harmful images, messages, and friends when certain keywords are tagged within the entry. Review flagged items to monitor who is contacting your children and advise them accordingly on further internet activity.



Likes and Privacy tabs reveal personal data fields that could be visible to anyone on Facebook

Useful Links

- A Parent's Guide to Internet Safety
- Microsoft Family Safety
- Net Nanny
- EyeGuardian

- www.fbi.gov/stats-services/publications/parent-guide
- <https://login.live.com>
- <http://netnanny.com/>
- <http://eyeguardian.com/>





EXIF Removal - Do's and Don'ts

- Prevent your phone from including geolocation data when capturing images.
- Remove EXIF data before sharing or posting images, especially images captured in private homes or businesses.
- Whenever possible, use a desktop EXIF viewer to verify EXIF data has been removed.
- 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. Instagram, Flickr).
- Even with no EXIF data, the content of images may contain identifying information, including persons and locations. Screen content with the assumption that anyone can see, copy, or forward photos 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 may utilize the information internally. EXIF data is stored as tags, some of which reveal unique identifying information.

Tag Category	Important Tags	Identity Implications
Geolocation	GPSLongitude, GPSLongitudeRef, GPSPLatitude, GPSPLatitudeRef, GPSDateStamp, GPSTimeStamp, GPSPAltitude, GPSPAltitudeRef, 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 log of behavior patterns and personal timeline.
Camera	Make, Model, SerialNumber	Unique serial number identifies the particular device for an image or sets of images.
Authorship	Artist, OwnerName, Copyright	Links image with a name or organization.
Image Summary	ImageDescription, UniquelImageID, UserComment	Potentially reveals identifying information about the content of the images, such as captured persons or 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 identifying EXIF data in image files and 2) Removing existing EXIF data from image files using an EXIF removal application.

Prevent the Capture of Geolocation Data

iOS (v6.0.1)

If iOS location services are turned off, images captured with the native iPhone camera app will not contain geolocation EXIF data.

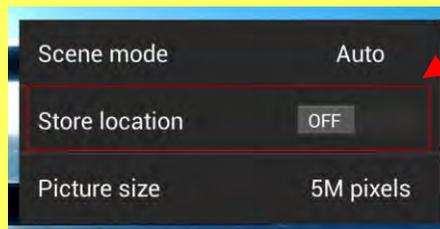
- 1 Select the *Settings* app on the iPhone home screen.
- 2 Navigate *Privacy>Location services*.
- 3 Turn off location services for the iPhone native camera application and any other image capture applications, such as Instagram.



Android (v4.2.1)

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 Hold the white circle in the bottom right corner to bring up a cluster of options in the middle of the screen. Click the settings symbol.
- 3 Slide the store location option to off.



Workarounds and Tips

- Taking a screenshot of a photo on a device running iOS 6 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 **contain geolocation data**. IBG recommends turning off location services/storage for your smartphone's camera application, as shown above.
- Remember that uploading or sharing a lower quality image will still **contain EXIF data**. EXIF data and image quality have no correlation.

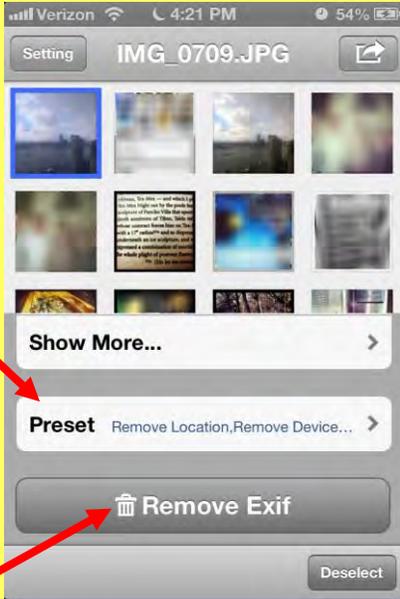


EXIF Removal Smartphone Apps

TrashEXIF for iOS

TrashEXIF is a free app that deletes geolocation and Camera 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 a photo(s) to clear of EXIF data.
- 3 Select *Presets*, then in the *Removal Presets* [sic] window, select *Remove Location* and *Remove Device Information*.
- 4 Return to the previous 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 with No EXIF is displayed as most recent in your iPhone Photo app.



PhotoInfo Eraser for Android

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

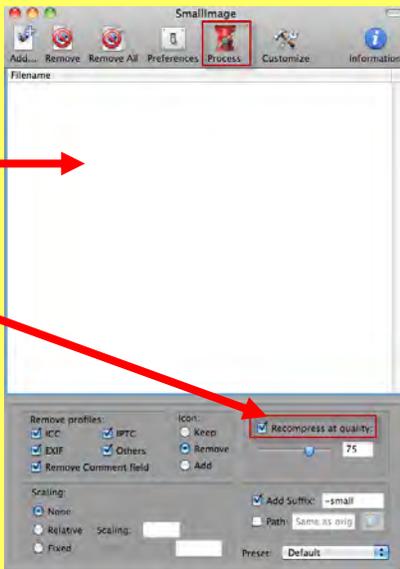
- 1 Download the PhotoInfo Eraser from the *Play Store*.
- 2 Open the PhotoInfo Eraser app and select *Gallery*.
- 3 Navigate your phone and select an image.
- 4 Select *Tag Delete* and press *OK*.
- 5 Navigate *Gallery*. A copy of your photo with no EXIF is now available in the *PIEraser* folder.



Viewing and Removing EXIF Data in OS X

Use the Small Image application (available at smallimage.en.softonic.com/mac) to remove EXIF data on your OS X device.

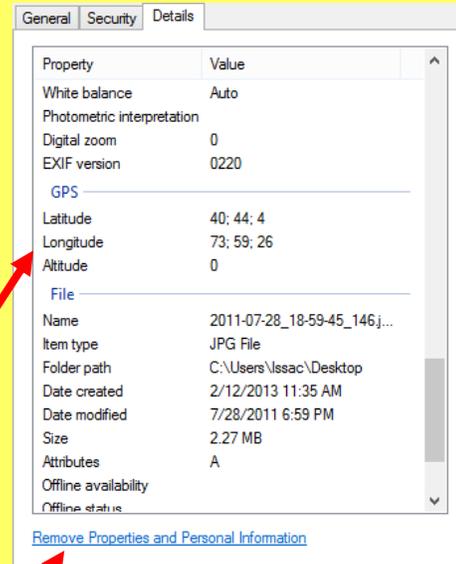
- 1 Open the Small Image application.
- 2 Drag the photos for EXIF removal into the application window.
- 3 Uncheck the *Recompress at quality* box.
- 4 Click *Process* to create a copy of the image with no EXIF data. (Uncheck the *Add Suffix* box to replace the original image file instead of creating a copy)
- 5 Check 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 Windows 8

Use the Windows 8 OS to verify EXIF data has been 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, is contained in the *Details* tab if it is included with the image.
- 4 Windows 8 also allows system administrators to remove all EXIF data from the selected image file by clicking the *Remove Properties and Personal Information* link.



Useful Links

A Parent's Guide to Internet Safety
Privacy Rights Clearinghouse
Microsoft Safety & Security
OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
www.privacyrights.org/fs/fs1-surv.htm
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx





Social Networks - 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 your face. 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, 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 has hundreds of privacy and sharing options. To control how your personal information is shared, you should use the settings shown below (such as *Only Me*, *Friends Only*) for (1) **Privacy**, (2) **Connecting**, (3) **Tags**, (4) **Apps/Websites**, (5) **Info Access through Friends**, and (6) **Past Posts**.

Control Your Default Privacy **1**

This setting will apply to status updates and photos you post to your profile from a Facebook app that doesn't have the inline audience selector, like the Facebook App for iPhone.

Change to "Friends Only"

Public Friends Custom

How You Connect

Control how you connect with people you know. [Edit Settings](#)

How Tags Work

Control what happens when friends tag you or your content. [Edit Settings](#)

Apps and Websites

Control what gets shared with apps, games and websites. [Edit Settings](#)

Limit the Audience for Past Posts

Limit the audience for posts you shared with more than friends. [Manage Past Post Visibility](#)

Block Lists

Manage your lists of blocked people and apps. [Manage Block Lists](#)

How You Connect **2**

Who can look up your profile by name or contact info? **Friends**

Who can send you friend requests? **Friends of Friends**

Who can send you Facebook messages? **Friends**

Who can post on your Wall? **Friends**

Who can see Wall posts by others on your profile? **Only Me**

[Learn more](#) [Done](#)

How Tags Work **3**

Profile Review of posts friends tag you in before they go on your profile (note: tags may still appear elsewhere on Facebook) **On**

Tag Review of tags that friends want to add to your posts **On**

Profile Visibility of posts you're tagged in once they're on your profile **Friends**

Tag Suggestions when friends upload photos that look like you **Off**

Friends Can Check You Into Places using the mobile Places app **Off**

[Done](#)

Choose Your Privacy Settings > Apps, Games and Websites **4**

Apps you use You're using 1 app, game or website: [Edit Settings](#)

Limit Use of Apps

How people bring your info to apps they use People who can see your info can bring it with them to apps. Use this setting to control the categories of info that can bring with them. [Edit Settings](#)

Uncheck ALL Boxes

Instant personalization Lets you see relevant information about you arrive on select partner websites. [Edit Settings](#)

Disable Personalization

Public search Show a preview of your Facebook profile using a search engine. [Edit Settings](#)

Disable Public Search

Info accessible through your friends **5**

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

<input type="checkbox"/> Bio	<input type="checkbox"/> My videos
<input type="checkbox"/> Birthday	<input type="checkbox"/> My links
<input type="checkbox"/> Family and relationships	<input type="checkbox"/> My notes
<input type="checkbox"/> Interested in	<input type="checkbox"/> Photos and videos I'm tagged in
<input type="checkbox"/> Religious and political views	<input type="checkbox"/> Hometown
<input type="checkbox"/> My website	<input type="checkbox"/> Current city
<input type="checkbox"/> If I'm online	<input type="checkbox"/> Education and work
<input type="checkbox"/> My status updates	<input type="checkbox"/> Activities, interests, things I like
<input type="checkbox"/> My photos	<input type="checkbox"/> Places I check in to

[Save Changes](#) [Cancel](#)

Limit The Audience for Old Posts on Your Profile **6**

If you use this tool, content on your profile you've shared with more than your friends (ex: Public posts) on your Wall will change to Friends. Remember: people who are tagged and their friends may see those posts as well.

You also have the option to individually change the audience of your posts. Just go to the post you want to change and choose a different audience.

[Learn about changing old posts](#) **Limit Old Posts to Friends Only** [Limit Old Posts](#) [Cancel](#)

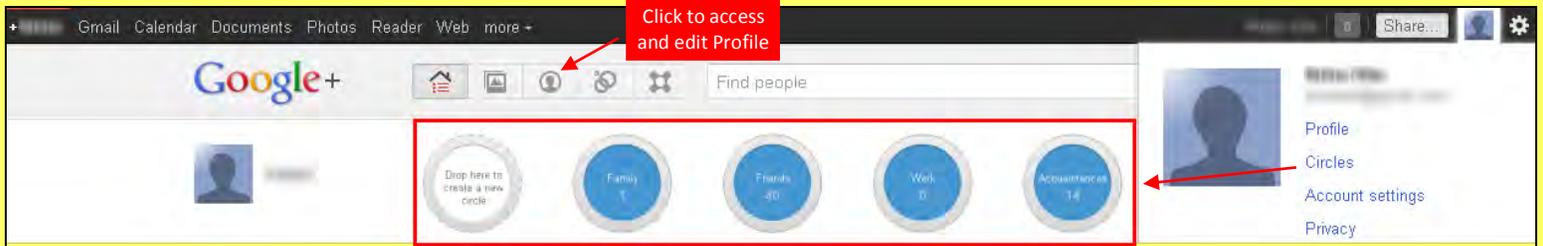


Social Networks - Do's and Don'ts

- 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 your face. 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, 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 Google+ Profile

Google+ provides privacy and sharing options using **Circles**. Circles are groups that users create for different types of connections, such as family, friends, or colleagues. Content is shared only with circles you select. Google+ requires that users provide real names - no pseudonyms.



Profile Settings

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

Click on the parts of your profile you want to edit. Done editing

Edit Profile (Select Edit Profile to make changes)

Uncheck both

Uncheck

Uncheck top button

Change to Only You

Change to Your Circles

Change to Your Circles

Uncheck

Search visibility (Help others find my profile in search results.)

This box is PUBLIC. Do not fill out additional information

Name & Profile Picture are PUBLIC

DO NOT add links to other online presences, such as a webpage, Facebook, Twitter, or LinkedIn

To share information on this page with specific people, select Custom then choose appropriate Circles

Click to access and edit Profile

Click to access and edit Profile

Drop here to create a new circle

Family

Friends

Work

Account settings

Profile

Circles

Account settings

Privacy

Send an email

In your circles (29)

Have in circles (23)

Change who is visible here

your circles

Show people in

Who can see this?

Anyone on the web

Your circles

Only you

Custom

Relationship

Looking for

Gender

Other names

Nickname

Search visibility

Not visible in search

Help others find my profile in search results.

Introduction

Bragging rights

Occupation

Employment

Education

Places lived

Links

Your circles

Save

Cancel

Who can see this?

Anyone on the web

Extended circles

Your circles

Only you

Custom

Your circles

Save

Cancel

Who can see this?

Custom

Type or select a circle or person. Or just enter an email address.

Friends (2)

Your circles

Extended circles

Public



Account Settings & Minimizing Your Activities

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

Google+

Who can interact with you and your posts

- Who can send you notifications? *Learn more* Your circles
- Who can comment on your public posts? *Learn more* Your circles
- Who can start a Messenger conversation with you? Circles

Notification delivery

Email: itsshelen@gmail.com

Phone: Add phone number **Don't Add Phone Number**

via Push notifications Don't notify me

Manage email subscriptions **Uncheck**

Occasional updates about Google+ activity and friend suggestions

- Account settings can be accessed under **Account Settings > Google+**.
- Maintain a small Google+ "footprint". Select only important Google+ notifications as shown in the box to the left.
- Limit notifications to email as opposed to text.
- **Do not** connect your mobile phone to Google+ or use the Google+ mobile application, and **Disable +1** on non-Google Websites
- **Do not** allow contacts to tag you then automatically link to your profile
- **Disable** your circles from accessing your photo tags prior to you

Google +1

+1 on non-Google sites Off Edit **Change to "Off"**

Google+ Pages

Automatically add a Google+ page to my circles if I search for + followed by the page's **Uncheck**

Photos

- Show photo geo location information in newly uploaded albums and photos. **Uncheck**
- Allow viewers to download my photos **Uncheck**
- Find my face in photos and prompt people I know to tag me. *Learn more* **Uncheck**

People whose tags of you are automatically approved to link to your Profile:
+ Add circles or people to share with... **Remove Everyone**

When a tag is approved, it is linked to your profile, and the photo appears in the "Photos of you" section.

Receive notifications **Check as indicated**

Notify me by email or SMS when someone...

Posts and mentions of my name Email Phone

- Mentions me in a post
- Shares a post with me directly
- Comments on a post I created
- Comments on a post after I comment on it

Circles Email Phone

- Adds me to a circle

Photos Email Phone

- Tags me in a photo
- Tags one of my photos
- Comments on a photo after I comment on it
- Comments on a photo I am tagged in
- Comments on a photo I tagged

Messenger Email Phone

- Starts a conversation with me

Connected accounts

You can improve your Google experience by connecting your accounts from other services.

Twitter Yes this is me No Suggested

Add this link to my public Google Profile, too **Uncheck**

Do not add outside accounts

Connecting your accounts

- When you search, you can see relevant content your friends share on the web.
- You make it easier for them to find the stuff you share on the web.
- You can choose which accounts to show on your public *Google Profile*.

Remember, Google won't share your searches or other private information with third-party services without your consent.

Use my Google contact information to suggest accounts from other sites. **Uncheck**

By default, Google+ uses your Google contact information to link your accounts from other online services, aggregating your online identity in one location. To disable this feature:

- Go to **Account Settings > Connected Accounts**
- Click "No" to Google-suggested 3rd-party accounts
- Disable Google+ access to your contact information
- Do not manually connect other online accounts using Google+

Deleting Your Google+ Profile Information or Account

Account overview

Services

- Delete profile and Google+ features
- Delete entire Google account
- View, enable, or disable web history

Delete profile and remove associated Google+ features

Close entire account and delete all services and info associated with it

Go to web history

Go to Account Settings > Account Overview

- **Delete Google+ Content** removes Google+ related information such as circles, +1's, posts, and comments
- **Delete your entire Google profile** removes all user data from Google services, including your Gmail
- **Disable web history** to prevent accumulation of your digital footprint

Useful Links

A Parent's Guide to Internet Safety
 Wired Kids
 Microsoft Safety & Security
 OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
www.wiredkids.org/
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx

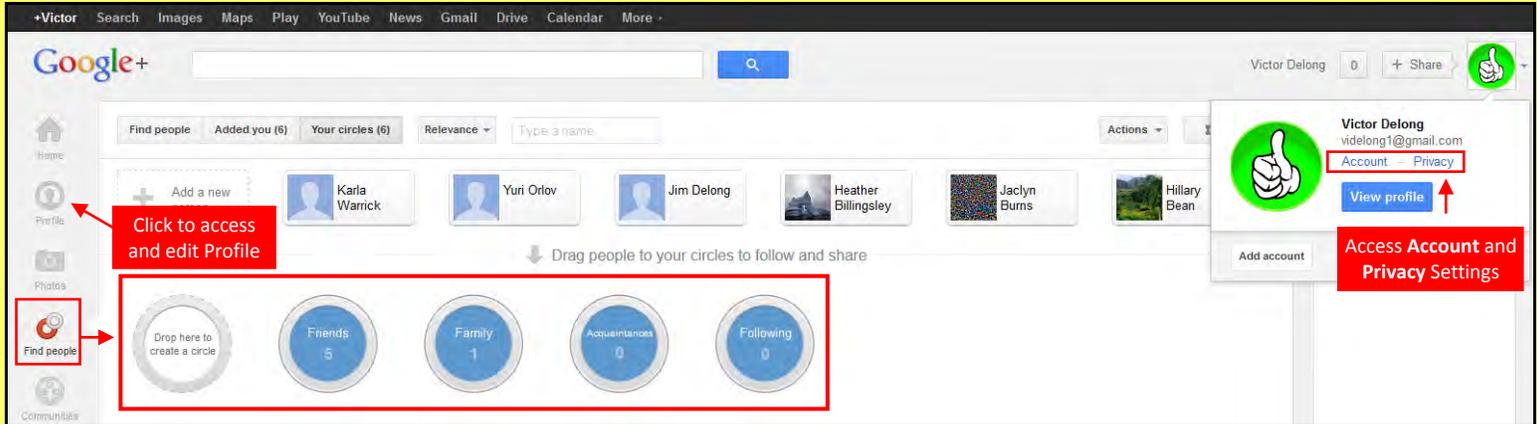


Social Networks - Do's and Don'ts

- 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 your face. 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, 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 Google+ Profile

Google+ provides privacy and sharing options using **Circles**. Circles are groups that users create for different types of connections, such as family, friends, or colleagues. Content can be shared publicly or only with circles you select. As of 2012, Google+ now allows pseudonyms.



Account Settings & Minimizing Your Activities

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

Account Settings

Who can interact with you and your posts

Who can send you notifications? [Learn more](#)

Who can comment on your public posts? [Learn more](#)

Change to Your Circles

Notification delivery

Email: videlong1@gmail.com

Phone: Add phone number

Do not add phone number

Go to Account > Google+ tab to change settings

Photos

Show photo geo location information in newly uploaded albums and photos.

Allow viewers to download my photos **Uncheck All**

Find my face in photos and videos and prompt people I know to tag me. [Learn more](#)

Upload my photos at full size.

Storage used: 0 GB (0%) of 5 GB. [Buy more storage](#)

Remove any names or circles from this field. Inspect each tag before linking it to your profile.

People whose tags of you are automatically approved to link to your Profile:

+ Add names, circles, or email addresses

Profile **Uncheck All**

Show your Google+ communities posts on your profile. [Learn more](#)

Only community members can see your posts, unless the community is public.

Show these profile tabs to visitors (they're always visible to you) [Learn more](#):

Photos

YouTube / Videos

+1

Reviews

Optional Fields. If activated, set to **Your Circles**.

Allow people to send you a message from your profile **Your circles**

Allow people to send you an email from your profile **Your circles**

Help others discover my profile in search results. [Learn more](#)

Google+ Pages **Uncheck**

Automatically add a Google+ page to my circles if I search for + followed by the page's name.

Location Settings **Uncheck**

Enable Location Sharing

Share your current location reported via background reporting on your devices with people you choose. [Learn more](#)

Who can see your best available location **Only you** **Never reveal location**

Deleting Your Google+ Profile or Google Account

Control what happens to your account when you stop using Google. [Learn more and go to setup](#) **Go to Account > Account Management for settings**

Delete profile and remove related Google+ features.

Close account and delete all services and information associated with it.

Other tools **Review**

[Go to the Dashboard to see all data stored in your account.](#)

[Manage connected accounts.](#)

[Manage your web history.](#)

- **Delete Google+ Content** removes Google+ related information such as circles, +1's, posts, and comments
- **Delete your entire Google profile** removes all user data from Google services, including your Gmail



Profile Settings

Click the **About** tab and apply the **Profile** settings shown below to ensure that your information is visible to only people of your choosing.

1 Never use a face photo. Name & Profile Picture & Cover Photo are always **PUBLIC**.

2 Allow Friends and Family Only.

2 Always Public. Do not include personal information in your tagline.

3 Cannot delete from profile.

3 Cannot delete from profile.

4 Uncheck.

1 In your circles: Show people in 2 circles. Who can see this? Public (selected), Your circles.

1 People: In your circles (7), Have you in circles (6).

2 Story: Tagline, Introduction, Bragging rights. Set changeable fields to Your Circles.

2 Education: Set all fields to Your Circles.

3 Basic Information: Gender, Looking for, Birthday, Relationship, Other names. Set all fields to Your Circles.

3 Links: Do not link to other SNS.

4 Apps: Uncheck Show apps card on your Google+ profile.

Work: Occupation, Skills, Employment. Set all fields to Your Circles.

Places: Do not enter location data.

Contact Information: Do not enter contact details.

Useful Links

A Parent's Guide to Internet Safety
 Privacy Rights Clearinghouse
 Microsoft Safety & Security
 OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
www.privacyrights.org/fs/fs18-cyb.htm
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx



Social Networks -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 your face. Select pictures taken at a distance, at an angle, or otherwise concealed. **Never post Smartphone photos**, 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 site whose users establish connections with co-workers, customers, business contacts, and potential employees and employers. Users 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.

LinkedIn Quick Facts

- There are over **200 million** LinkedIn users around the world. It is widely adopted in the US, India, Canada, and the UK.
- Users tend to share information related to their **careers or jobs** as opposed to photographs from social events.
- LinkedIn profiles tend to be more **visible and searchable** than other social networks such as Facebook and Twitter.
- Compared to free accounts, **Paid LinkedIn accounts** have access to more information about other users viewing their profile.
- Approximately 42% of LinkedIn users update their profile information on a regular basis.





Account Settings

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

A screenshot of the LinkedIn Account Settings menu. The 'Account' option is highlighted with a red box. A red arrow labeled '1' points to 'Manage Advertising Preferences' and another red arrow labeled '2' points to 'Manage security settings'. The menu items include: Profile, Email Preferences, Groups, Companies & Applications, Account, Privacy Controls, Manage Advertising Preferences, Settings, Change your profile photo & visibility, Show/hide profile photos of other members, Customize the updates you see on your home page, Select your language, Manage security settings, Email & Password, Add & change email addresses, Change password, Helpful Links, Upgrade your account, Close your account, and Get LinkedIn content in an RSS feed.

Passwords

Use a complex password with capital letters and numbers to ensure that attackers cannot access your account information. Change your password every 6 months to maximize security.

Closing Your LinkedIn Account

If you no longer plan to use the LinkedIn service, you can close your account. Click **Close your account** and confirm that you want to take this action.

A screenshot showing two settings panels. The top panel is 'Manage Advertising Preferences' (labeled '1') with the 'LinkedIn may show me ads on third-party websites' checkbox unchecked. A red box with an arrow points to this checkbox with the text 'Uncheck the box. Opt out of partner advertising on third party websites'. The bottom panel is 'Security settings' (labeled '2') with the checkbox 'When possible, use a secure connection (https) to browse LinkedIn' checked.

Protecting Your Data

If you frequently access LinkedIn through public WiFi, enable the https security setting to encrypt your data.

Application Settings

Third-party applications and services can access most of your personal information once you grant them permission. Limit your use of applications to ensure that third parties cannot collect, share, or misuse your information. Apply the **Groups** and **Applications** settings shown below to ensure that your information is visible only to people of your choosing.

A screenshot of the LinkedIn 'Groups, Companies & Applications' settings page. The 'Groups, Companies & Applications' menu item is highlighted with a red box. Red arrows labeled '1', '2', and '3' point to 'Turn on/off notifications when joining groups', 'Turn on/off data sharing with 3rd party applications', and 'Manage settings for LinkedIn plugins on third-party sites' respectively.

A screenshot of the 'Data sharing with third-party applications' settings page. The checkbox 'Yes, share my data with third party applications' is unchecked. A red box with the text 'Uncheck the box. Do not share with third parties.' is overlaid on the page.

Avoid using Twitter connect and the LinkedIn smartphone app to prevent accidentally sharing location data or personal information.

LinkedIn retrieves information about users on websites with LinkedIn Plug-In integration and reports comprehensive summaries of its users through the Bing search engine. Prevent sharing your activities on third-party websites with LinkedIn to protect your online identity.

A screenshot of the 'Notifications when joining groups' settings page. The checkbox 'Yes, publish an update to my network whenever I join a group that has these notifications enabled by the group owner.' is unchecked. A red box with the text 'Uncheck the box. Prevent automatic posting.' is overlaid on the page.

A screenshot of the 'Manage settings for LinkedIn plugins on third-party sites' settings page. The checkbox 'Yes, allow LinkedIn to receive information about my visits to pages that use LinkedIn plugins.' is unchecked. A red box with the text 'Uncheck the box. Do not share with third parties.' is overlaid on the page.

Useful Links

A Parent's Guide to Internet Safety
Privacy Rights Clearinghouse
Microsoft Safety & Security
OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
<https://www.privacyrights.org/privacy-basics>
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx





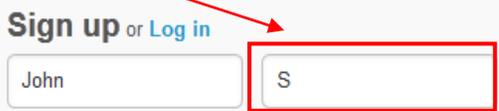
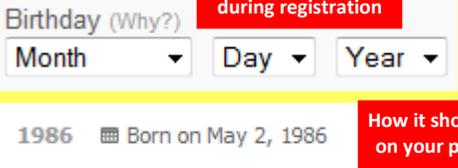
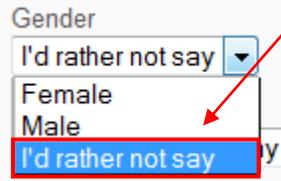
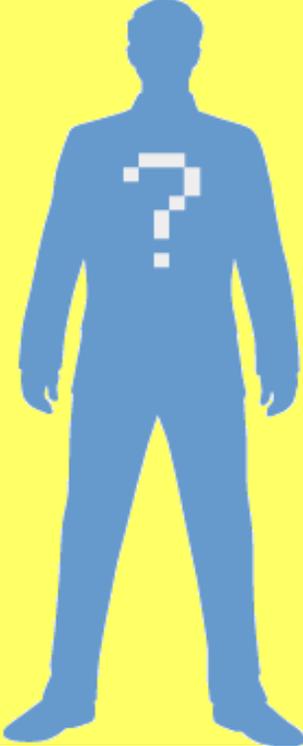
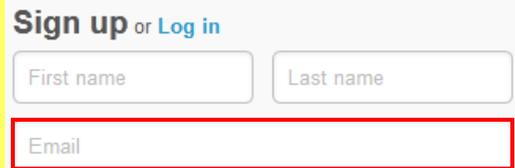
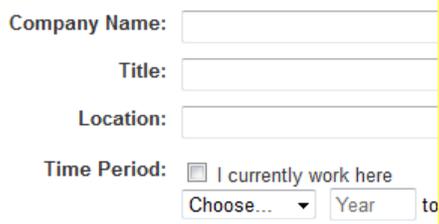
Online Registration Smart Card

Online Registration - Do's and Don'ts

- Research online services to make sure that they are legitimate before giving them identity information.
- Avoid filling in optional identity fields for online services; only fill in the minimum required identity information.
- Never give online services access to your social security number or physical address.
- When possible, use a username instead of a real name on online services.
- 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 online services.

Identity Elements of Social Networking Site (SNS) Accounts

Online identity can be described as an aggregate of accounts and account-related activities associated with a single person. Below identifies common identity elements that are required by social networking services for creating accounts and participating in their online services.

<p>First and Last Name</p> <p>First and last name are mandatory for almost all SNS accounts. In order to better protect yourself, use the initial of your last name instead of its full version, especially if you have an unusual last name.</p> 	<p>Username & Password</p> <p>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.</p> <p>DO NOT use the same password across your SNS accounts. Use unique password for each of your accounts.</p>	<p>Birthday</p> <p>Birthdays are used to verify user's age and customize age-appropriate content for the user on the site. This information is sometimes published on the SNS profile and has to be removed retroactively.</p> 
<p>Gender</p> <p>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.</p> 		<p>Email Address</p> <p>Email is the 2nd most common requirement for creating a SNS account. It is used to verify your account during registration, as well as using it as the credential name for your future log-ins.</p> 
<p>Location: Address, Zip Code, Country</p> <p>Location information is required at varied levels of granularity depending on the service. It may include address, zip code, and/or country.</p> 		<p>Company / Employment Information</p> <p>Company and employment information are required for professionally-oriented SNS services, where the main purpose is to meet and build your network with other people in your field.</p> 
<p>Facebook Account</p> <p>Many third party websites have adapted Facebook's authentication platform, Facebook Connect. Signing up with Facebook enables users to create new accounts by importing information that already exists on Facebook. Some sites require this process.</p> 		<p>Twitter Account</p> <p>As with Facebook, Twitter accounts have become a popular mode of creating new SNS accounts on other services. Your Twitter username and password are used as your authentication, instead of email and password.</p> 



Online Registration Smart Card

Identity Information Required During Registration by Services

	LinkedIn	Facebook	Twitter	Google+	Yahoo!	MSN	Foursquare	Pinterest	OkCupid
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
Country	x			x	x	x			x
Company / Employment Info	x								
Job Title	x								
Zip code	x				x	x			x
Facebook Account							optional	optional	
Twitter Account							optional	optional	
Sexual Orientation									x
Relationship Status									x

Or sign-up for a new Windows Live Account

Increasing numbers of SNS services use existing Facebook or Twitter

Online Registration and Verification Process

1 Enter required identity fields on the registration page.

Sign Up
It's free and always will be.

First Name: John
Last Name: Smith
Your Email: Jsmith10@gmail.com
Re-enter Email: Jsmith10@gmail.com
New Password:
I am: Male
Birthday: Jan 1 1989

By clicking Sign Up, you agree to our Terms and that you have read and understand our Data Use Policy, including our Cookie Use.

Sign Up

Identity fields are filled out by the user

2 Confirm your account via email or mobile phone. Avoid using mobile verification unless required by the service you are signing up.

facebook

Hi John,

To complete the sign-up process, please follow this link:
<http://www.facebook.com/confirmemail.php?e=johnsmith70777%40gmail.com&c=63192>

You may be asked to enter this confirmation code: 63192

Welcome to Facebook!
The Facebook Team

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

Get started:
Complete Sign-up

Confirmation link sent to your email. Follow the link to complete registration

3 Finish the confirmation process on the service website.

Account Confirmed

You have successfully confirmed your account with the email johnsmith70777@gmail.com.

Okay

Final confirmation received on the social networking site online

Useful Links

A Parent's Guide to Internet Safety
Privacy Rights Clearinghouse
Microsoft Safety & Security
OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
<https://www.privacyrights.org/privacy-basics>
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx





Opting Out of Public Records and Data Aggregators – Best Practices

- 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.

What to Look For

Search for your name, names of family members, email addresses, phone numbers, home addresses, and social media usernames. Once you have located information that you want removed, you should save your findings to facilitate the removal process. The information presented about how to remove personal details from data aggregators is subject to change.

PrivateEye – Veromi – USA People Search

PeopleFinders – PublicRecordsNow



- www.privateeye.com
- www.publicrecordsnow.com
- www.veromi.com
- www.peoplefinders.com
- www.usa-people-search.com

PrivateEye, Veromi, PeopleFinders, and PublicRecordsNow are all owned by the same parent company, Confi-Chek.com. Sending one opt-out and including a letter referencing all five companies should remove you from all of them. To opt out you'll have to mail a letter containing four printed documents:

- (1) your records that you found
- (2) a list of the information you want removed
- (3) a copy of your ID
- (4) a letter requesting removal

Send the letter to:

Opt-Out
1821 Q Street
Sacramento, CA 95811

Information to be removed (part 2 above) should contain the following:

- Service you intend to opt out of (e.g. PrivateEye)
- First name, last name, middle initial
- Aliases and A.K.A.'s
- Complete current address and former addresses going back 20 years
- Date of birth (month, day, and year)

PeopleSmart



www.peoplesmart.com

You can do a special opt-out search on PeopleSmart. If you find your information, click 'That's the one!' In step 1, fill in both email fields. Skip all the other fields. In step 2, select the radio button next to "Hide everything." All of the fields below will fill in automatically. Fill in the case-sensitive CAPTCHA, click 'Yes,' and submit.

Intelius – Zabasearch – Public Records – Spock – iSearch PeopleLookUp – PhonesBook – DateCheck – LookupAnyone

- www.intelius.com www.publicrecords.com
- www.zabasearch.com www.lookupanyone.com
- www.peoplelookup.com www.phonesbook.com

Intelius owns, or is affiliated with, the following people search websites: Zabasearch, Public Records, Spock, iSearch, PeopleLookUp, PhonesBook, DateCheck, and LookupAnyone. When you request removal of your records, you should also request removal from this network of sites. You can opt-out of Intelius either online (at www.intelius.com/optout.php) or by fax. You can fax your ID and a letter containing the information you want removed to **425-974-6194**, using the following cover sheet:



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

Wink – MyLife



- www.wink.com
- www.mylife.com

Wink is owned and operated by MyLife, so the same opt-out instructions apply. 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 them that you want your listing removed and provide the specific information that you want deleted. Be sure to specifically mention that you want to be removed from Wink.com as well as MyLife.com. Once they confirm removal, the listing will be off the site in 7-10 days.

Whitepages



www.whitepages.com

Search for your information on the website 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, edit the information so that it does not represent truthful information. Additionally, check the box under "Hide" and hit the update button to finalize changes.



Public Records and Data Aggregators Smart Card

Opt Out Smartcard 060513_1656

BeenVerified



www.beenverified.com

Send an email to support@beenverified.com with the

subject "Opt Out Request" using this template:

Dear BeenVerified Customer Support:

As per your privacy policy, please permanently remove my listing from your databases:

- Your name as shown on the site:
- Your age:
- Your current address (city, state, zip):
- Previous addresses:
- Listed relatives:
- The copy and pasted URL of the Been Verified search results page where you found your information:

Thank you for your assistance.

You'll receive 2 confirmation emails: the first to confirm they received your request, and the second several days later to confirm that they removed your listing.

123People



www.123people.com

Locate your listing on the website, then visit their opt-out page. Fill in your first name, last name, email, title, country, language, and the CAPTCHA to complete the opt-out. An email will be sent to you right way providing links back to 123People used to mark specific information for deletion. Select the garbage can next to any of the information belonging to you and submit a request for deletion. The site will delete your information within 48 hours after verification.

Lookup.com



www.lookup.com

Search for your listing on the website. You can identify a listing by the blue and black circle icon to the left of the listing. Other search sites' information is aggregated below, but it does not count as a Lookup profile.

Next, open their opt-out page. Fill in first name, last name, the URL of the Lookup profile you found for yourself, email, phone, and address to complete the opt-out request.

US Search



www.ussearch.com/consumer/ala/landing.do?did=590

Enter first name, middle initial, last name, city, state, age, and click 'GO' to search for yourself on USSearch's special Privacy Lock page. Select the correct result and click 'This is the record I would like to block.' Save the record page(s) as a PDF. Fax the record page(s) & your ID to **425-974-6242** using the following template:

As per your privacy policy, please remove this listing from your site. Thank you for your help with this personal security issue.

Useful Links

- | | |
|------------------------------|---|
| Abine Online Privacy | https://www.abine.com/optouts.php |
| OPSEC Awareness | http://www.slideshare.net/JIOWCOS/opsec-awareness-data-aggregation |
| Privacy Rights Clearinghouse | https://www.privacyrights.org/fs/fs1-surv.htm |
| Optout Protect Your Identity | http://www.optout.com/ebook/ebook7.aspx |



PeekYou



www.peakyou.com

Search for yourself on the website. If you find a listing, go to their opt-out page. Fill in the required fields, and under 'Actions,' select 'Remove my entire listing.' Under "Reason for removal," select whichever applies to you. Paste the numbers at the end of your profile's URL in the 'Unique ID' field, fill in the CAPTCHA, and you're all set.

You'll get an immediate email confirming that you've sent in your opt-out and a second email up to a few days or weeks later to tell you it's been deleted.

PeopleFinder



www.peoplefinder.com

Search for yourself on the website. If you find a listing, go to their opt-out page.

Enter your first name, last name, city, state, zip code and address or phone number. Choose your removal reason from the drop-down and enter the code number. You do NOT need to provide your email to remove yourself.

Spoke



www.spoke.com

Search for yourself on Spoke and click the 'This is me' button. On the next page, look for the 'To suppress your profile, click here' link on the right side of the page and follow the directions. Be sure to click the removal link in the email you provide to complete the process.

Spokeo



www.spokeo.com

Search for your information on the website. If you find yourself (and you may have more than one listing) open up Spokeo's opt-out page. Repeat the removal process for each listing, and be sure to click the link in each confirmation email you receive to finish the opt-out.

USIdentify



www.usidentify.com

First, see if you're listed by searching for yourself on the website. If you are, send the following info with a printout of what you want removed to:

Opt-Out/USIdentify.com
1030 E HWY 377 Ste 110-213
Granbury, TX 76048

Information to be removed should contain the following:

- First name, last name, middle initial
- Aliases and A.K.A.'s
- Complete current address
- Complete former addresses going back 20 years
- Date of birth (month, day, and year)



Photo Sharing Services Smart Card

Photo Sharing - 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.
- Ensure that your family takes similar precautions with their photos; their privacy and sharing settings can expose your images.
- Avoid posting or tagging images that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Do not use your face as a profile photo, and do NOT enable Location Services for your smartphone camera or photo sharing app.

Choosing the Right Photo Sharing Service

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

- Are you sharing photos primarily for yourself, your friends and family, or for public consumption?
- Are your contacts or viewers already using a specific service?
- How much control do you need to maintain over your images? Is the retention of EXIF data problematic?

Your choice of photo sharing service determines the amount of control you retain over your images. All services allow you to remove images, but not all services allow for account deletion. However, deleting your content or your account does not ensure removal from the Internet.

Nine popular photo sharing services are described below. Default settings are in bold.

Service	Primary Use	Image Privacy Options	Keeps EXIF?	Location Adding Options (non-EXIF)	Allows Reposting?	Google Indexed?
	Share photos within grouped user environments	Private, Contacts, Family, Friends, Public	Yes, No	Editable location, map based	Yes, No	If Public (can opt-out)
	Social Network	Only Me, Friends, Friends of Friends, Public	No	Free-form text, linked to Facebook page, map based	Yes	If Public
	Share photos from camera enabled mobile devices	Requests to follow must be approved, Public	No	GPS-based device location; Customizable location, text search	No	No
	Share photos publicly or privately	Public , Private (optional password protection)	Yes, No	None	Yes	If Public
	Social Network	Only you, Circles , Public	Yes	Editable location, map based	Yes	If Public
	RSS Feed	Requests to follow must be approved, Public	No	Non-editable GPS location for mobile; Text selection for website (city, state)	Yes	If Public
	Enhanced photo sharing in Twitter	None , based on Twitter	Yes, No	Website-based location, or GPS-based for smartphone	Yes	If Public
	Enhanced photo sharing in Twitter	None , based on Twitter	No	None	Yes	If Public
	Share concepts and ideas using images	Public	Yes	None	Yes	Yes

Instructions for restricting visibility, searchability, and location data retention for each photo sharing service are provided below.

Flickr – Allows detailed control over photo sharing

In the upper left of the page go to *You >> Your Account >> Privacy & Permissions*. Set as follows:

- Allow others to share your stuff? *No*
- Who can add you to a photo? *Only You, edit >> Remove me from all photos*
- Allow your stuff to be added to a gallery? *No*
- Hide your EXIF data? *Yes*
- Show which application you used for uploading? *No*
- Hide your stuff from public searches? *edit >> Yes to all three*
- Who will be able to see, comment on, add notes, or add people? *Friends and Family*
- Who will be able to see your stuff on a map? *Only you*
- Import EXIF location data? *No*

Facebook – Compresses images & deletes EXIF, increasing privacy

Go to *Privacy Settings*.

- Set Who can see your future posts = *Friends*
 - Limit the audience for old posts on your timeline
- 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? *On*
 - 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*

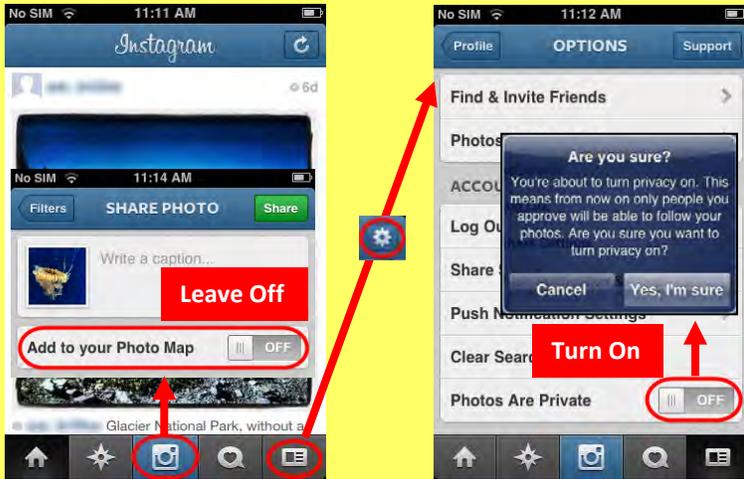




Photo Sharing Services Smart Card

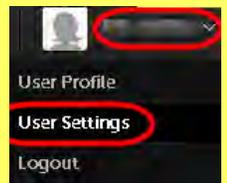
Instagram – Closed network,

Follow these pictographic instructions for Instagram on the iPhone:



Photobucket – Allows for password-protected sharing

In the upper right go to *User Settings*. On the *Albums* tab, uncheck all options listed under *Links* except *Link back to albums*.



On the *Privacy* tab set as follows:

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

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

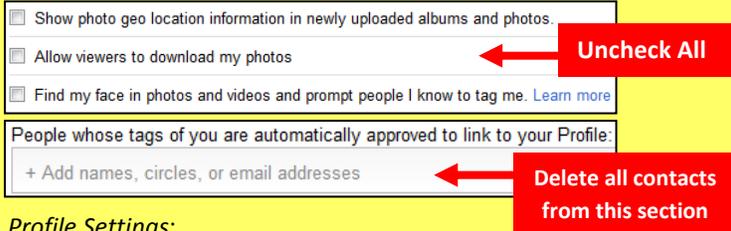
- *Make Private – Only you can view, or*
- *Password Protect – Anyone with the URL link and the password can view*

Remember, choose unique passwords for each album

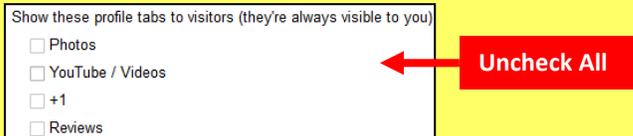
Google+ – Retains all EXIF, multiple privacy settings

Navigate *Settings* >> *Google+* and apply the following Settings.

Photo Settings:



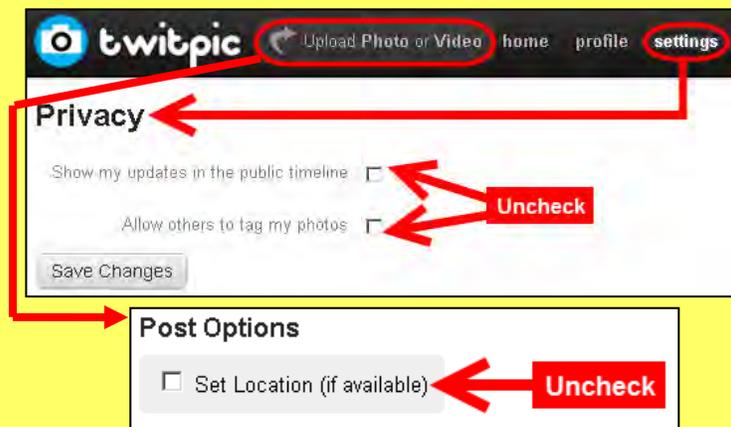
Profile Settings:



Location Settings: disable location sharing and set to *Only You*

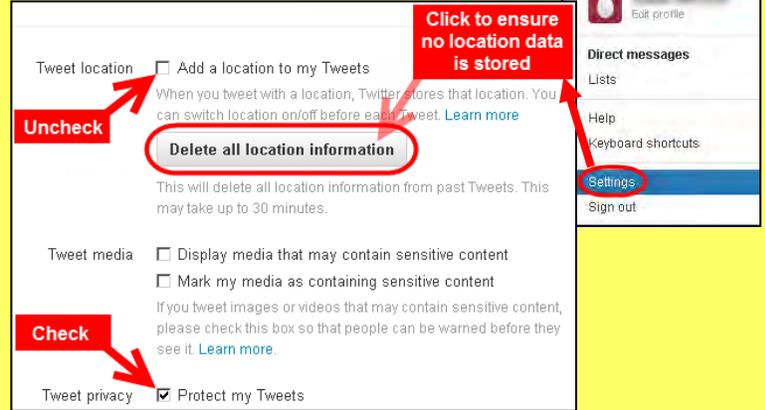
Twitpic – Retains EXIF, privacy settings limited

Twitpic posts links to photos on Twitter. Twitter's privacy settings should be used in conjunction with the native security settings below. Follow these browser-based pictographic instructions for Twitpic:



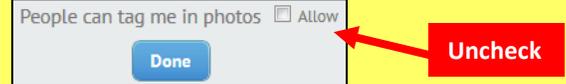
Twitter – Removes EXIF, but minimal options to limit visibility

In the upper right go to *Settings*. Once on the *Settings* page, set indicated options as shown.



Yfrog Services – Removes EXIF, privacy settings very limited

Yfrog can be used to post links to photos on Twitter and has also become its own social network called Yfrog Social. When using Yfrog with Twitter, go to *Settings* and disable photo tagging.

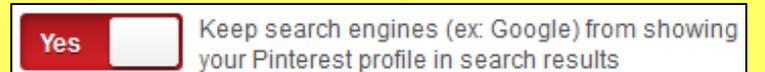


When using Yfrog Social navigate *Settings* >> *Account Info* and set the profile to *private*. Individual privacy settings can also be chosen for each picture and album during upload.



Pinterest – Retains EXIF, privacy settings very limited

In the upper right go to *Settings* under the drop down menu. Under *Basic Information* turn *Search Privacy On*.



Useful Links

U.S. Army Social Media Roundup
 Washington State Web Wise
 Microsoft Safety & Security
 OnGuard Online

- <http://dmna.ny.gov/members/geotagging.pdf>
- <http://www.atg.wa.gov/InternetSafety/SharingOnline.aspx>
- <http://www.microsoft.com/security/online-privacy/location-services.aspx>
- <http://www.onguardonline.gov/articles/0033-heads>





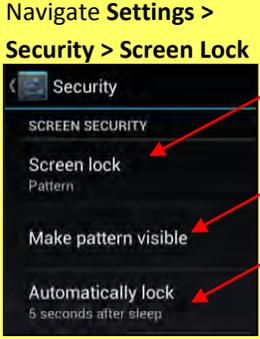
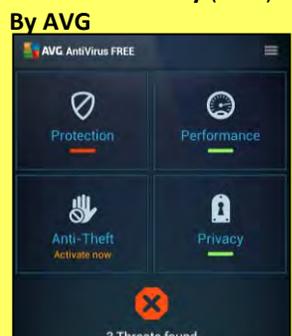
Smartphone Smart Card

Smartphone -Do's and Don'ts

- Malicious individuals may gain physical access to your smartphone. 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 near classified information, and remove the battery before discussing any sensitive information.
- Wireless networks may be insecure and subject to monitoring. Use VPN when accessing wireless networks, and do not access sensitive information over wireless networks. Turn off Bluetooth when you are not using it to prevent hackers from exploiting your device.
- Apps that you download may gain access to the data stored on your smartphone. Check to see if the app will access your personal data and read user reviews of the app to see if other users experienced trouble after downloading.
- Apps can track your location. Turn off location services to avoid unwanted location tracking.

Physical Access and Malware Threats

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

Threat	iPhone 6.1.3	Android 4.1.2
<p>Physical Access Threats – To prevent others from accessing data on your smartphone, set up a passcode to protect your information. Android has multiple passcode styles including pattern, PIN, password, and face recognition while the iPhone uses alpha-numerical codes and PINs.</p>	<p>Navigate Settings > General > Passcode Lock</p>  <p>Create a complex password containing letters and numbers</p> <p>Block Access</p> <p>Optional Setting</p>	<p>Navigate Settings > Security > Screen Lock</p>  <p>Use a password or pattern. Avoid using face recognition.</p> <p>Uncheck</p> <p>Always auto-lock your devices</p>
<p>Lost or Stolen Phones - It is reported that on average 113 cell phones will be stolen every minute in the United States. Download apps such as Find My iPhone or Android Lost to locate, lock, or control your data remotely. These apps allow users to manage data on their smartphones from internet webpages accessed via desktop or portable device.</p>	<p>Find My iPhone (Free)</p>  <p>Capabilities:</p> <ul style="list-style-type: none"> • Remote Lock • Erase Data • GPS Locator • Sound Alarm • Send Text Message to Phone • Backup Data Through iCloud Storage 	<p>Android Lost (Free)</p>  <p>Capabilities:</p> <ul style="list-style-type: none"> • Remote Lock • Erase Data • GPS Locator • Sound Alarm • Send Text Message to Phone • Activate Camera • Read Texts Sent • View Call List
<p>Malware – Your smartphone is vulnerable to malware from emails, websites, and downloaded apps. Between 2011 and 2012 alone, smartphones had an increase in malware attacks by over 1,200% with Android being the most susceptible. Download third-party security apps such as Virusbarrier and AVG's Antivirus Security to prevent malware from stealing your information.</p>	<p>Virusbarrier (\$0.99)</p>  <p>iPhones are not readily susceptible to viruses. Use this app to prevent passing malware to your contacts.</p> <p>Capabilities:</p> <ul style="list-style-type: none"> • Scan for spyware, adware, and Trojans • Scan emails and PDF files before sending 	<p>Antivirus Security (Free) By AVG</p>  <p>Capabilities:</p> <ul style="list-style-type: none"> • App Scanner • File Scanner • Website Scanner • Text and Call Blocker • Remote Lock • Erase Data Remotely • GPS Locator • Kill Slow Tasks

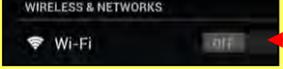
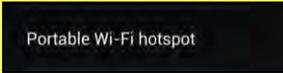
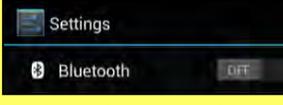
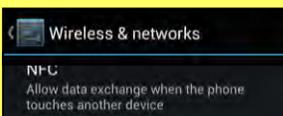
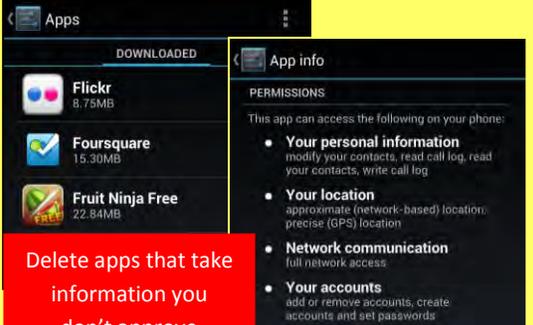
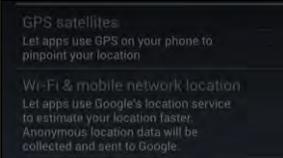
Best Practices

- 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 manufacturer and 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.



Smartphone Smart Card

Wireless Connections and App Security Settings

Threat	iPhone	Android
<p>Wireless Networks – Information transmitted via public Wi-Fi networks can be intercepted by third parties. Avoid using public wireless networks when possible and always use a VPN client to encrypt your online transactions.</p>	<p>Navigate Settings > Wi-Fi</p>  <p>Disable Wi-Fi when not in use</p>  <p>Enable Network Permissions</p> <p>Navigate Settings > General > VPN to enable and establish a VPN connection</p>	<p>Navigate Settings > Wi-Fi to manage connections</p>  <p>Disable Wi-Fi when not in use</p> <p>Navigate Settings > More > Tethering & Portable Hotspot and disable Portable Wi-Fi Hotspot</p>  <p>Uncheck</p> <p>Navigate Settings > More > VPN to enable and establish a VPN connection</p>
<p>Bluetooth – Bluetooth involves the wireless communication of two devices within a close proximity. When Bluetooth is enabled, hackers may be able to access the connection to your device and retrieve your contacts, calendars, emails, messages, and photos without your knowledge. Avoid using Bluetooth and disable it when it is not being used.</p>	<p>Navigate Settings > Bluetooth to disable services</p>  <p>Disable Bluetooth when not in use</p> <p>Navigate Settings > Personal Hotspot to disable broadcasting a personal internet connection.</p>  <p>Never share your internet connection</p>	<p>Navigate Settings > Bluetooth to disable services</p>  <p>Disable Bluetooth when not in use</p> <p>Navigate Settings > More > NFC to manage Near Field Communications settings which can be used to transfer data via touching devices together.</p>  <p>Uncheck</p>
<p>Data Retaining Apps – Downloaded applications frequently collect users' 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.</p>	<p>Navigate Settings > General > Siri</p>  <p>Disable Siri</p> <p>Navigate Settings > Privacy to view and manage which apps are using specific information.</p>  <p>Turn Off</p>	<p>Navigate Settings > Apps and review individual apps to see what information is being collected</p>  <p>Delete apps that take information you don't approve</p>
<p>Location Threats – The majority of apps will ask permission to track your current location. Users should avoid granting permission to these apps when possible and turn off all location tools when they are not in use. It is also important to note that pictures taken with smartphones retain location information within EXIF data. Never upload pictures taken from your smartphone to social networking sites.</p>	<p>Navigate Settings > Privacy > Location Services</p>  <p>Only grant access to apps that require a location to function</p> <p>Disable location services when not in use</p>	<p>Navigate Settings > Location Access</p>  <p>Uncheck when location services are not in use</p>  <p>Only grant access to apps that require a location to function</p>

Smartphone Useful Links

<p>A Parent's Guide to Internet Safety Microsoft Safety & Security OnGuard Online Privacy Rights Clearinghouse</p>	<p>www.fbi.gov/stats-services/publications/parent-guide www.microsoft.com/security/online-privacy/social-networking.aspx www.onguardonline.gov/topics/social-networking-sites.aspx www.privacyrights.org/fs/fs2b-cellprivacy.htm#smartphonedata</p>  <p>A NOVETTA SOLUTIONS COMPANY www.ibgweb.com</p>
--	---



Traveling Safely With Smartphones

Traveling with Smartphones - Do's and Don'ts

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

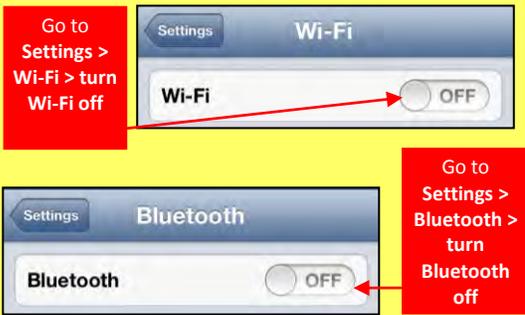
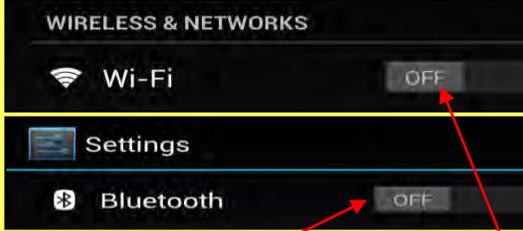
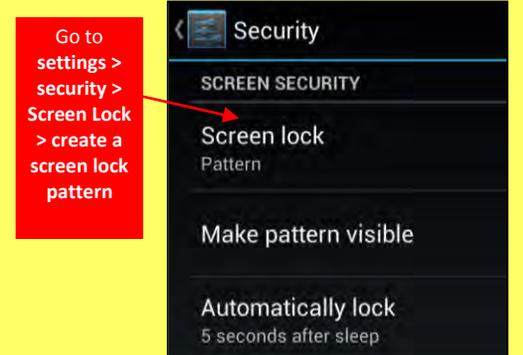
To Do When Traveling	iPhone	Android
<p>Ensure that your phone's software is up to date – Use apps to ensure that the software on your smartphone is up to date.</p>	<p>Go to Settings > General > Software Update</p> <p>Check to see if your software is up to date; if not, your phone will prompt you to download the latest software</p>	<p>Go to Settings > About Phone > System Updates</p> <p>Check to see if your software is up to date; if not, your phone will prompt you to download the latest software</p>
<p>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.</p>	<p>Use the Lookout app for iPhone Go to Security > Process Monitor to see if malicious processes are running on your iPhone</p>	<p>Use the AVG Antivirus FREE app for Android Click Scan Now to scan for viruses</p>
<p>Set your phone to lock automatically – In case you lose your device, you want your smartphone to lock automatically to prevent physical access.</p>	<p>Go to settings > General > Auto-Lock Set the Auto-Lock to 1 Minute</p>	<p>Go to settings > Display > Sleep Set the phone to sleep after 1 minute</p> <p>Go to settings > Security > Automatically Lock Set to lock immediately after sleep</p>



Traveling Safely With Smartphones

Traveling with Smartphones – 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 a more secure alternative to saving information locally

To Do When Traveling	iPhone	Android
<p>Disable Wi-Fi and Bluetooth – Disable Wi-Fi and Bluetooth on your smartphone; Wi-Fi and Bluetooth can render your smartphone vulnerable to malware and hacking.</p>	 <p>Go to Settings > Wi-Fi > turn Wi-Fi off</p> <p>Go to Settings > Bluetooth > turn Bluetooth off</p>	 <p>Go to Settings > Bluetooth > turn Bluetooth off</p> <p>Go to Settings > Wireless & Networks > turn Wi-Fi off</p>
<p>Use a 10+ character password or Screen Lock Pattern – short passwords are vulnerable to brute force attacks. Chose a password with a combination of letters, numbers, and symbols. If using a Screen Lock Pattern, choose a complicated pattern.</p>	 <p>Enter a new passcode with 10+ characters, symbols, and numbers</p> <p>Go to Settings > Passcode Lock > Turn Off Simple Passcode</p>	 <p>Go to settings > security > Screen Lock > create a screen lock pattern</p>
<p>Recover lost or stolen smartphones and wipe data – Find my iPhone and Cerebus can locate lost devices and wipe data remotely from lost or stolen smartphones.</p>	 <p>Use the Find My iPhone app to recover lost or stolen iPhone smartphones</p>	 <p>Use the Cerebus app to recover lost or stolen Android Smartphones and wipe data remotely from the device memory and SD card</p>



Social Networks -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 your face. 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, 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 microblogging site whose users send and read text-based posts online. The site surged to worldwide popularity with +500 million active users as of 2012, generating 55 million Tweets and 1.6 billion search queries daily.

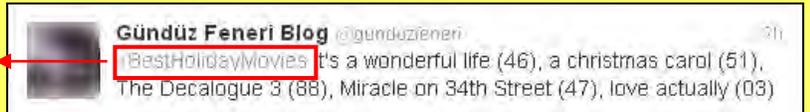


Following are people you subscribe to
Followers subscribe to your tweets
Private Tweets will only be visible to followers you approve

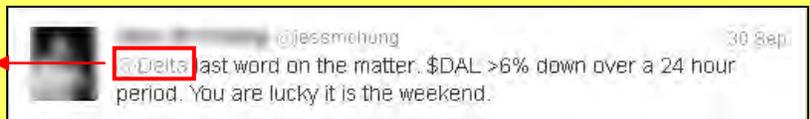
Tweets

"Tweets" are short text-based messages – up to 140 characters – that users post to Twitter. "Tweet" can refer to a post as well 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 mark a keyword or topic in a Tweet. Posts with hashtag are categorized by topics in the Twitter search engine. Hashtagged words that become popular become Trending Topics (ex. #jan25, #egypt, #sxsw).

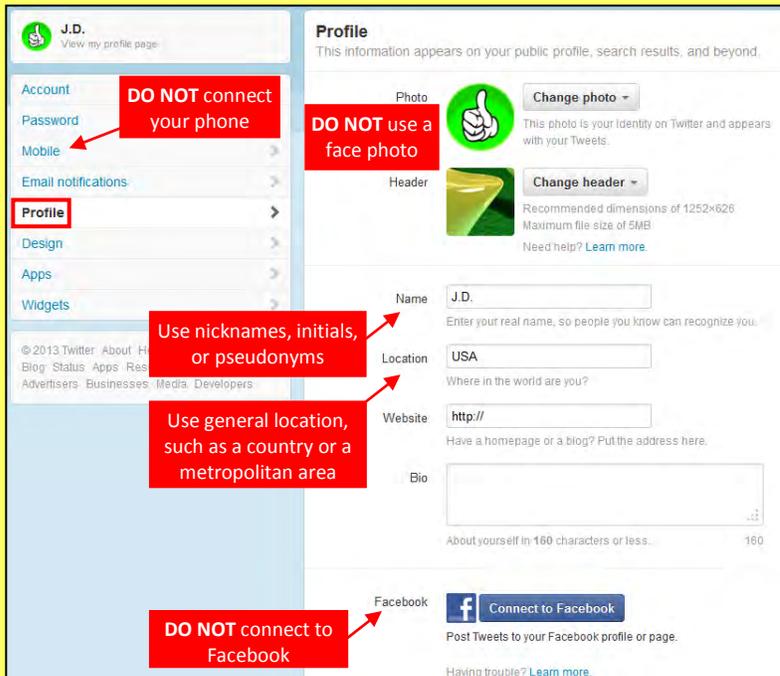


Mentions (@username) are used to tag a user in a Twitter update. When a public user mentions a private Twitter account, the link to the private account profile becomes public.



Profile Settings

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



Twitter Best Practices

- Avoid using hashtags (#) in updates to avoid being indexed and associated with a topic by Twitter Search.
- *Tweet responsibly.* Do not provide personal details regarding your whereabouts and activities in your post.
- Do NOT upload links to personal photos or websites on Twitter.
- Do NOT allow Twitter to use your location on mobile devices.
- Change your Twitter **username** frequently to limit your account exposure.



Account Settings

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

Account

Change your basic account, language, Tweet privacy, and location settings.

Username Change every ~6 months
<https://twitter.com/Delong1JW>

Email
 Email will not be publicly displayed. [Learn more.](#)
 Let others find me by my email address Uncheck

Language ▼
 Interested in helping translate Twitter? Check out the [Translation Center.](#)

Time zone ▼

Tweet location Add a location to my Tweets Uncheck
 When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. [Learn more](#)
 Click to delete all location data associated with your account
 This will delete all location information from past Tweets. This may take up to 30 minutes.

Tweet media Display media that may contain sensitive content
 Mark my media as containing sensitive content
 If you tweet images or videos that may contain sensitive content, please check this box so that people can be warned before they see it. [Learn more.](#)

Tweet privacy Protect my Tweets Check
 Your Tweets are currently protected. Only those you approve can access your Tweets. Your future Tweets will be visible to the public. Tweets posted previously may still be visible in some places. [Learn more.](#)
Protecting your Tweets makes all your posts private. Only those who you approve can access your tweets.

Personalization Tailor Twitter based on my recent website visits Uncheck
 Preview suggestions tailored for you (not currently available to all users). [Learn more](#) about how this works and your additional privacy controls.
 Do Not Track Check
 While you have Do Not Track turned on, your visits to sites that feature Twitter are not available to personalize your experience.

Password reset Require personal information to reset my password Check

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

Your pending follower requests

Jess M Chung @jessmchung
 I spend a lot of time thinking about all the things I'd buy or eat. That and complaining.

Deactivating / Delete Your Twitter Account

To deactivate your account, go to **Settings** and select **Account**. At the bottom of the page, click **"Deactivate my account."** After deactivation, the user can reactivate the account within **30 days**. After 30 days, the account is permanently **deleted**.

Notification & Application Settings

Maintain a small digital footprint by minimizing the number of notifications. Revoke access to unnecessary third party applications.

Email notifications

Control when and how often Twitter sends emails to you. [Learn more.](#)

Activity related to you and your Tweets

Email me when My Tweets are marked as favorites
 Private Tweets cannot be retweeted

My Tweets are retweeted Check
 ▼

My Tweets get a reply or I'm mentioned in a Tweet Check
 ▼

Someone sends me a follow request
 I'm sent a direct message Direct messages are never visible to the public
 Someone shares a Tweet with me
 Someone from my address book joins Twitter

Activity from your network

Email me with Top Tweets and Stories
 ▼
 Updates about activity from my Twitter network

Updates from Twitter

Email me with News about Twitter product and feature updates Twitter updates may highlight new security tools or possible risks
 Tips on getting more out of Twitter
 Things I missed since I last logged into Twitter
 News about Twitter on partner products and other third party services
 Participation in Twitter research surveys
 Suggestions about people I may know on Twitter
 Suggestions based on my recent follows

Applications

These are the apps that can access your Twitter account. [Learn more.](#)

Photos on iOS by Apple® Learn how to revoke an iOS app.
 Whether you're flicking through an album or zooming in to see the smallest detail, you'll be amazed at how sharp, vibrant, and beautiful your photos look. And so will everyone you show them to.
 read and write access
 Approved: Sunday, March 11, 2012 9:57:28 PM

iOS 5 by Apple®
 iOS 5 Twitter integration
 read and write access
 Approved: Sunday, March 11, 2012 9:56:33 PM

Useful Links

A Parent's Guide to Internet Safety
 Privacy Rights Clearinghouse
 Microsoft Safety & Security
 OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
www.privacyrights.org/fs/fs18-cyb.htm
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx