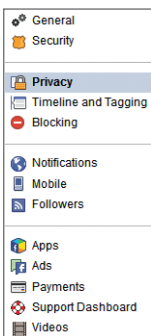




Social Network - Do's and Don'ts

- 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 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.

Privacy Settings



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

Facebook interactions such as likes and wall posts have been effectively used to classify individuals. Try to minimize the amount of personal information that you post on social networking services.

1 Under **Privacy**, limit the audience for future posts in the **Who can see your future posts?** feature. Review all activity by clicking **Use Activity Log**. Hide individual posts from your timeline or set to **Friends** or **Only Me**. You can change previously posted content shared with friends of friends or the public to friends only by clicking **Limit Past Posts**. This also allows you to control who can contact or look you up.

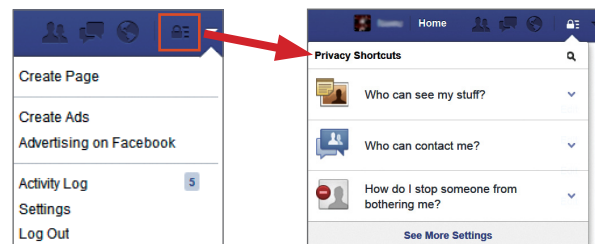
Who can see my stuff?	Who can see your future posts?	Custom	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
	Whose 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 Click **Timeline and Tagging>View As** to see what your profile will look like to the public or to a specific user.

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

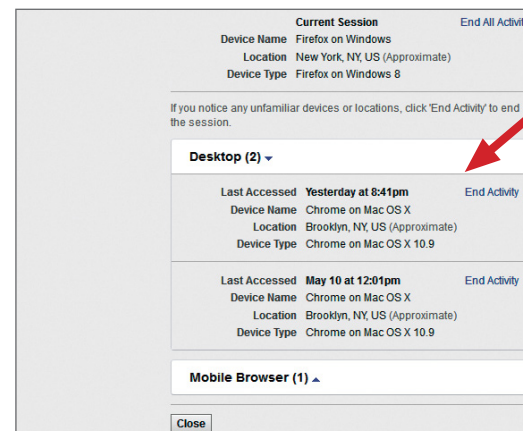
Do not login or link third-party sites (e.g. Twitter, Tinder) using your Facebook account. "Facebook Connect" shares your information and your friends information with third party sites that may aggregate, misuse, or disseminate personal information. Additionally, Facebook apps, such as Farmville, access and share your personal data. Use as few of these apps as possible.

Minimizing Your Facebook Profile



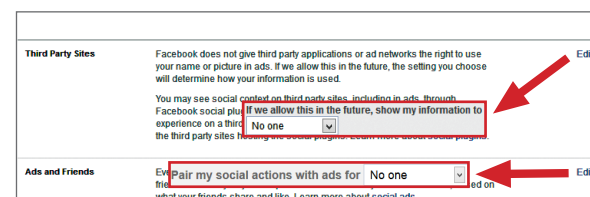
Facebook has privacy shortcuts to basic settings to limit what others can see in your profile, accessible using the **lock** icon. For more extensive settings, click the **triangle** icon then **Settings**. From there navigate pages from the side toolbar to control how your personal information is shared.

3 As a safety precaution, navigate **Security Settings>Where You're Logged In** and click **End Activity** for sessions no longer in use.

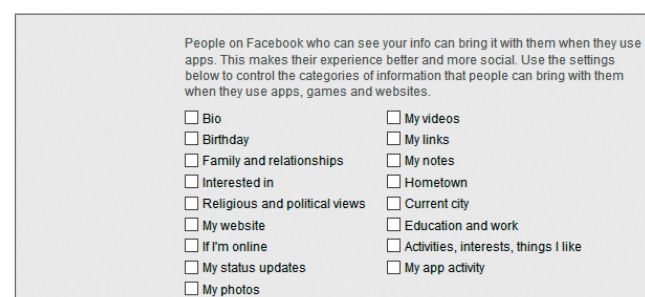


End activity for unrecognized locations and devices

4 Set **Third Party Sites** and **Ads & Friends** fields to 'No one' to prevent third party sites from using your name or picture for ads in the future.



5 Facebook permits other users to share your data through apps. Navigate **Apps>Apps others use** to limit the information fields others can distribute during their Facebook use.





Timeline Settings

Click **About** on your profile page and apply the settings shown to ensure that your information is visible to only people of your choosing. Each field, such as **Relationships and Family**, **About You**, **Favorite Quotations**, **Living**, **Basic Information**, and **Contact Information** has an **Edit** option. Limit each of these fields to a more exclusive privacy setting, typically 'Friends' or the most exclusive setting, typically 'Only Me.'

The Facebook mobile app's privacy settings are identical to those on the website and are located under the **More>Settings** menu. **Privacy Shortcuts** are also available in the mobile app.

However, smartphones' GPS features can further expose users. If you are using an iOS device navigate to **Settings>Privacy>Location Services** and turn off location services for the Facebook app.

Even with location services disabled, Facebook allows you to **Check-In** to common locations. Do not utilize this feature.

Manage Your Contacts

Under the **Friends** tab:

- Navigate **Edit>Edit Privacy** to change who can view your contacts limit your contact list to 'Only Me.'
- Navigate **Edit>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.

Deactivating/Deleting Your Facebook Account

Deleting Accounts

How do I permanently delete my account?

If you **deactivate** your account, your Timeline disappears from the Facebook service immediately. People on Facebook won't be able to search for you, though some info, like messages you sent, may still be visible to others. We also save your Timeline information (ex: friends, photos, interests) in case you want to **come back**.

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

If you can't log into your account, you'll need to reset your password first. To do this, go to www.facebook.com and click the **Forgot your password?** links below the password field. Once you've followed the instructions to reset your password and can log into your account, you can deactivate or delete your account using the steps outlined above.

To deactivate your Facebook account, go to **Settings** and select **Security**. To reactivate your account log in to Facebook with your address and password.

To delete your Facebook account, go to **Help** from the triangle icon 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 remove your data 14 days after a security check.

Useful Links

A Parent's Guide to Internet Safety
Privacy Rights Clearinghouse
Microsoft Safety and Security
Online Guardian

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



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 and friends 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.



Home

Profile

People

Photos

Communities

Events

Hangouts

Pages

Local

Settings

Account Settings & Minimizing Your Activities

Apply the Account settings shown with arrows below to ensure that your information is shared in a limited fashion. Use **Your circles** settings to choose which circles you share with when sharing a post with 'all circles.'

Your circles

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

Customize

Photos and Videos

- ☐ Show geo location information on newly uploaded photos and videos.
- ☐ Allow viewers to download my photos and videos.
- ☐ Find my face in photos and videos and prompt people I know to tag me. [Learn more](#)

Uncheck
All

Hashtags

- ☐ Add related hashtags from Google on my newly created posts. [Learn more](#)

Google sometimes adds hashtags to posts. Uncheck to prevent hashtags from being included. This makes you less visible."

Google Drive

- ☐ Show Drive photos and videos in your photo library [Learn more](#)
Only you can see them in your library until you choose to share them

Uncheck

Location Settings

Uncheck

- ☐ Enable Location Sharing

Location Sharing allows you to share your current location from Location Reporting on your devices, with people you choose. People you share your location with can see your current location across Google products, including Google+ and Google Now. They can also see your places, such as home and work. [Learn more](#)

Google allows you to opt-out of Google+. This does not delete your Gmail or other Google services functionality."

Disable Google+

Delete your entire Google profile [here](#).

Profile Settings

Click the About tab and Edit (within the **People** card). This pops up the editing window. Edit all cards by using the navigation buttons. You have multiple options to limit the visibility of your information.

- **Public**--can be seen by anyone (not recommended)
- **Extended circles**--can be seen by people in circles of people in your circles (not recommended)
- **Your circles**--can be seen by anyone included in your circles (minimum privacy recommendation)
- **Custom**--allows you to limit who or which circles can view the information (intermediate privacy recommendation).
- **Only you** (maximum privacy recommendation)



Profile Settings

People

In your circles

☐ Show people in **All circles**

Who can see this?

☒ Public

☐ Your circles

Have you in circles

☐ Show people who have added you to circles

Cancel **Save**

Uncheck "Show people in and Show people who have added you to their circles"

Story

Tagline **Public**

A brief description of you

Introduction **Only you**

Bragging rights **Only you**

Examples: survived high school, have 3 kids, etc.

Cancel **Save**

Work

Occupation **Only you**

What do you do?

Skills **Only you**

What are your skills?

Employment **Only you**

Employer name Job title

Start - End ☐ Current

Cancel **Save**

Education

Education **Only you**

School name Major or Field of study

Start - End ☐ Current

Description of courses

Cancel **Save**

Places

Places lived **Only you**

type a city name ☐ Current

Cancel **Save**

Do not enter place names

Basic Information

Gender **Male** **Only you**

Looking for **Only you**

☐ Friends

☐ Dating

☐ A relationship

☐ Networking

Birthday **January** **23** **1990** **Only you**

☐ Show birthday year

Relationship **I don't want to say** **Only you**

Other names **Only you**

For example: maiden name, alternate spellings

Cancel **Save**

Contact Information

Home **Only you**

Phone New contact info

Work **Only you**

Phone New contact info

Cancel **Save**

Do not enter or display phone number information

Links

Other profiles **Only you**

[Add custom link](#)

[Manage connected accounts](#)

Contributor to **Only you**

[Add custom link](#)

Links **Only you**

[Add custom link](#)

Cancel **Save**

Apps with Google+ Sign-in

Apps with Google+ Sign-in **Only you**

☐ Show this card on your Google+ profile

change who can see your signed-in apps and activities on Google services, [change app settings](#)

Cancel **Save**

Uncheck

Useful Links

A Parent's Guide to Internet Safety
Privacy Rights Clearinghouse
Microsoft Safety and Security
Online Guardian

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

NOVETTA
www.novetta.com

Instagram smart card

Personal safety tips

- ✓ 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.
- ✓ Use caution when posting images of you or your family. Be aware of your surroundings, to include identifiable locations, military affiliations, and any other personal security vulnerabilities.
- ✓ It's highly discouraged to use geo-location tags.
- ✓ Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Security tips

Here are 5 things you can do to help keep your account safe:

- ✓ Pick a strong password. Use a combination of at least six numbers, letters and punctuation marks (like ! and &).
- ✓ Make sure your email account is secure.
- ✓ Log out of Instagram when you use a computer or phone you share with other people.
- ✓ Think before you authorize any third-party app.
- ✓ Never give up your password to someone you don't know and trust.

Privacy and safety tips

Decide whether you want to use your 'Photo Map'.

Adding location to photos, also known as using the 'Photo Map' feature, is turned off for all photos someone uploads to Instagram. This means that photos won't appear on a person's Photo Map without their permission.

Block if necessary

When people use Instagram's blocking feature, the person they block cannot view their posts or search for their Instagram account.

Make your posts private

You can make your posts private in the Instagram app so only approved followers can see them.

Things to keep in mind about private posts:

- ✓ Private posts you share to social networks may be visible to the public depending on your privacy settings for that network. For example, a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your Twitter posts.
- ✓ Once you make your posts private, people will have to send you a follow request if they want to see your posts, your followers list or your following list.
- ✓ You'll see requests in Activity, which you can then approve or ignore.
- ✓ People can send a photo or video directly to you even if they're not following you.



Remember

- ✓ Your media represents you. That probably seems obvious, but remember it can keep on representing you well into the future, because content posted online or with phones is pretty impossible to take back. So it's a good idea to think about how what you post now will reflect on you down the line. If you think it might hurt a job prospect, damage a relationship or upset your grandmother, consider not sharing it.
- ✓ Your media could show up anywhere. Even if you limit the audience, be careful not to share anything that could be a problem if someone were to pass it around. **Once it's on the internet, it's there forever!**

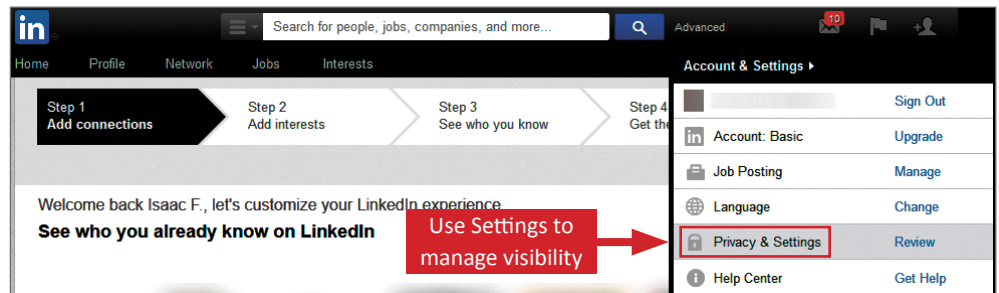


Social Network - Do's and Don'ts

- 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 and friends 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 LinkedIn Profile

LinkedIn is a professional networking site that allows you to establish connections with co-workers, customers, business contacts, and potential employees and 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.

Profile	Privacy Controls	Settings
	1 Turn on/off your activity broadcasts	Manage your Twitter settings
	2 Select who can see your activity feed	Manage your WeChat settings
	3 Select what others see when you've viewed their profile	Helpful Links
	4 Turn on/off How You Rank	Edit your name, location & industry >
	5 Select who can see your connections	Edit your profile >
	Change your profile photo & visibility >	Edit your public profile >
	6 Show/hide "Viewers of this profile also viewed" box	Manage your recommendations >
	Manage who you're blocking >	

Uncheck

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.

Your connections

Set to Only You

3 What others see when you've viewed their profile

- ☐ Your name and headline (Recommended)



Technical Consultant at
Greater New York City Area

- ☐ Anonymous profile characteristics such as industry and title

Note: Selecting this option will disable Profile Stats. Whenever you switch to anonymous, your viewer history gets erased.



Someone at

- ☒ You will be totally anonymous.

Set to totally anonymous

Note: Selecting this option will disable Profile Stats. Whenever you switch to anonymous, your viewer history gets erased.

4 Turn on/off How You Rank

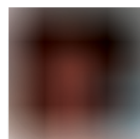
How You Rank shows how you compare to your connections and colleagues in terms of profile views. If you turn this feature off, others won't see you or your standings in their How You Rank page. You also won't see your own rank or get tips on improving your visibility.

- ☐ Let others see how you rank

Uncheck

5 Who can see your connections

Current Photo



Edit Photo

Delete Photo

Upload a Photo

You can upload a JPG, GIF or PNG file (File size limit is 4 MB).

Browse...

No file selected.

Upload Photo or Cancel

By clicking "Upload Photo", you certify that you have the right to distribute this photo.

In addition to users I message, my profile photo is visible to...

- ☒ My Connections
☐ My Network
☐ Everyone

Do not use a photo of your face for your account

Use Settings to manage visibility

6 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 300 million LinkedIn users around the world. The service is widely adopted in the US, India, Canada, and the UK.
- Users tend to share information related to their careers or jobs, not photographs from social events.
- Compared to free accounts, paid LinkedIn accounts have access to more information about other users viewing their profile.
- 48% of users invest 0-2 hours/week on LinkedIn, however a sizable portion of the community, 26% spends 3-4 hours/week and 26% spends more than 4 hours/week.



Accounts Settings

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

The screenshot shows the LinkedIn Account settings menu. The 'Account' option is highlighted with a red box. A red arrow points from the 'Account' option to the 'Manage security settings' link. Another red arrow points from the 'Manage security settings' link to the 'Close your account' link in the 'Email & Password' section.

- Profile
- Communications
- Groups, Companies & Applications
- Account

Privacy Controls

- 1 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
 - 2 Manage security settings

Email & Password

- Add & change email addresses
- Change password
- Helpful Links
 - Upgrade your account >
 - Close your account >

Passwords

Use a long, random passwords with capital letters and numbers to ensure that attackers cannot access your account information. Change your password every six months to maximize security.

Closing Your LinkedIn Account

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

Manage Advertising Preferences 1

Ads by LinkedIn - Overview

"Ads by LinkedIn" are advertisements shown to LinkedIn ... [Read more](#)

Ad selection

Ads shown to you are selected based on non-personally ... [Read more](#)

Protecting your personal information

LinkedIn does not directly share your personal information ... [Read more](#)

- ☐ LinkedIn may show me ads on third-party websites.
- ☐ LinkedIn may show me ads based on third party data.

Check secure connection

Set up two-factor verification

Uncheck

Security Settings 2

Secure connection

☐ A secure connection will be used when you are browsing LinkedIn. [Learn More >](#)

Note: Some LinkedIn applications will not be available when you select this option.

Two-step verification for sign-in

Turning this feature on will sign you out anywhere you're currently signed in. We will then require you to enter a verification code the first time you sign in with a new device or LinkedIn mobile application. [Learn More >](#)

Currently OFF • Turn On

Note: Some LinkedIn applications will not be available when you select this option.

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.

Avoid using Twitter connect and the LinkedIn smartphone app to prevent accidentally sharing location data or personal information. LinkedIn retrieves information about your activity on websites with LinkedIn Plug-In integration and reports comprehensive summaries through the Bing search engine. Do not allow the sharing of your activities on third-party websites with LinkedIn.

The screenshot shows the LinkedIn Groups, Companies & Applications settings menu. The 'Groups, Companies & Applications' option is highlighted with a red box. A red arrow points from the 'Groups, Companies & Applications' option to the 'Turn on/off data sharing with 3rd party applications' link. Another red arrow points from the 'Turn on/off data sharing with 3rd party applications' link to the 'Manage settings for LinkedIn plugins on third-party sites' link.

- Profile
- Communications
- Groups, Companies & Applications
- Account

Groups

- Select your group display order >
- View your groups >
- Set the frequency of group digest emails
- Turn on/off group invitations
- 1 Turn on/off notifications when joining groups
- Companies
 - View companies you're following >

Applications

- View your applications >
- Add applications >
- Privacy Controls
 - 2 Turn on/off data sharing with 3rd party applications
 - 3 Manage settings for LinkedIn plugins on third-party sites

Notifications when joining groups 1

☐ Yes, publish an update to my network whenever I join a group that has these notifications enabled by the group owner.

Uncheck

Data sharing with third-party applications 2

☐ Yes, share my data (including basic profile and contact information) with third party applications.

Save changes or Cancel

Uncheck

Manage settings for LinkedIn plugins on third-party sites 3

If you're signed in to LinkedIn when you view any page that uses our professional plugins, we receive information that you've visited that page. This allows us to improve your LinkedIn experience and provide you with insights from your professional network, like how many of your connections have shared an article into LinkedIn using the Share on LinkedIn plugin.

☐ Yes, allow LinkedIn to receive information about my visits to pages that use LinkedIn plugins.

Uncheck

Useful Links

A Parent's Guide to Internet Safety
Privacy Rights Clearinghouse
Microsoft Safety and Security
Online Guardian

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

NOVETTA
www.novetta.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 an 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 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 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, GPSLatitude, GPSLatitudeRef, GPSTimeStamp, 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 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 and navigate *Privacy > Location Services*.

2 Turn off location services altogether or for the iPhone's camera applications.

3 Return to the *Settings* app and navigate *Privacy > Photos*.

4 Disable the permissions for other apps to have access to the photos stored in the device's camera roll.

Location Services Off

Camera Off

Camera+ Off

FaceR Off

魔镜 Off

Google+ Off

Android (v4.3)

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 the 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.

MORE OPTIONS

Location icon disabled

Prevent 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 contain geolocation data. Novetta 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.

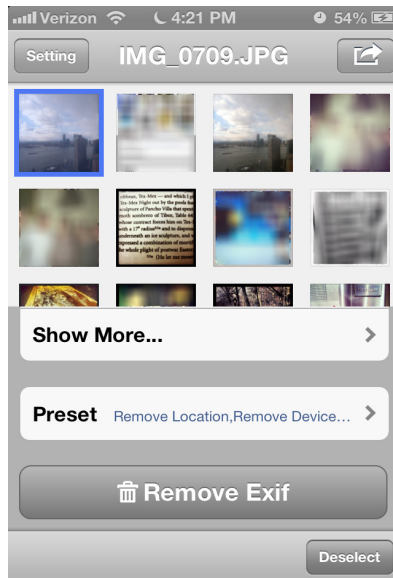


EXIF Removal Smartphone Apps

TrashEXIF for iOS

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

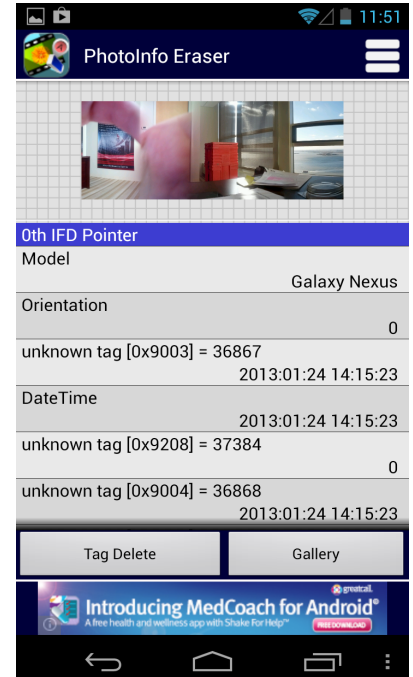
- 1 Download the TrashEXIF app from the *App Store*.
- 2 Open the TrashEXIF app and select a photo(s) to clear of EXIF data.
- 3 Select *Presets*, then in the *Removal Presets* [sic] window, select *Remove Location* and *Remove Device Information*.
- 4 Return to the previous screen by clicking the name 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.

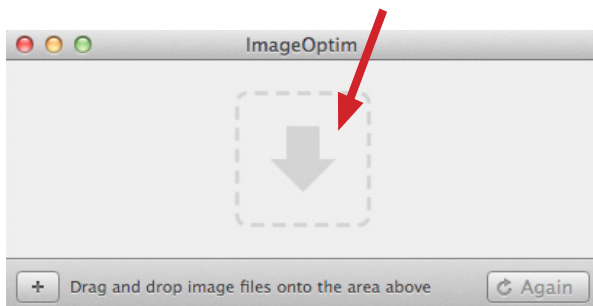
- 1 Download the PhotoInfo Eraser from the *Play Store*.
- 2 Open the PhotoInfo Eraser app and select *Gallery*.
- 3 Navigate your phone and select an image.
- 4 Select *Tag Delete* and press OK.
- 5 Navigate *Gallery*. A copy of your photo with no EXIF is now available in the *PIEraser* folder.



Viewing and Removing EXIF Data in OS X

Use the ImageOptim application (available at <http://imageoptim.com/>) to remove EXIF data on your OS X device.

- 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.

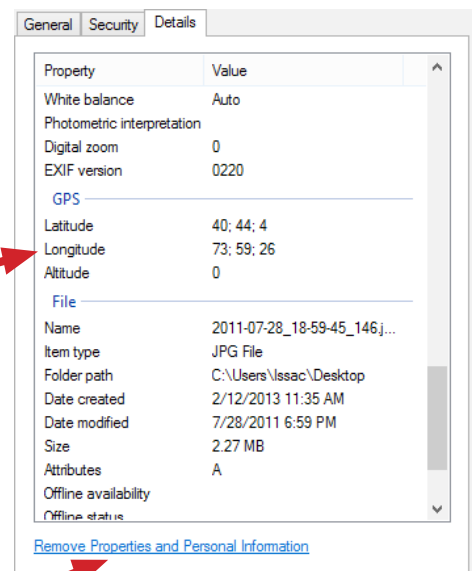


- 3 Check that the EXIF data has been removed by right-clicking the image and select *Get Info*. EXIF data is listed under *More Info*.

Viewing and Removing EXIF Data in 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 and Security
Online Guardian

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

NOVETTA
www.novetta.com





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 and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show 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. As of June 2014, the site has approximately 230 million daily active users, generating 500 million Tweets and 2.1 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

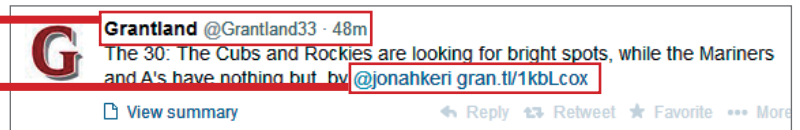


Tweets

"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 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.

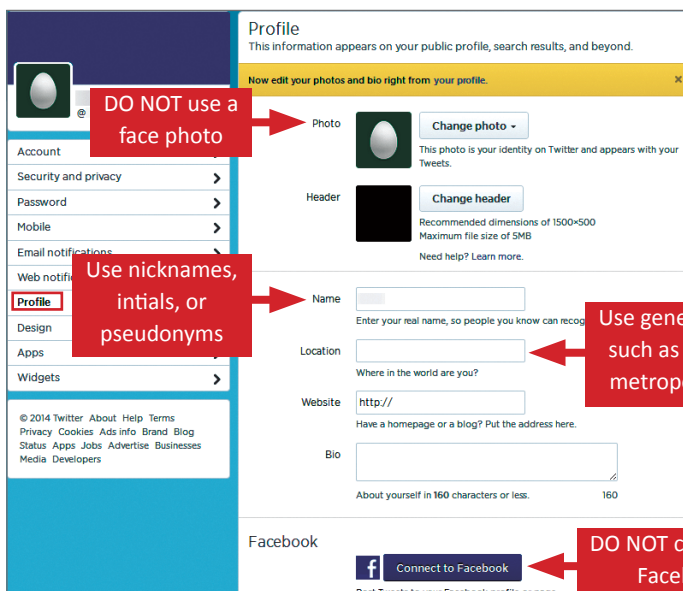
Mentions (@username) are used to tag a user in a Twitter update. When a public user mentions a private Twitter account, the link to the private account profile becomes public.

Hashtags (#topic) are used to mark a keyword or topic in a Tweet. Posts that include a hashtag are categorized by topics in the Twitter search engine. Hashtagged words that become popular are Trending Topics (ex. #jan25, #egypt, #sxsw).



Profile Settings

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

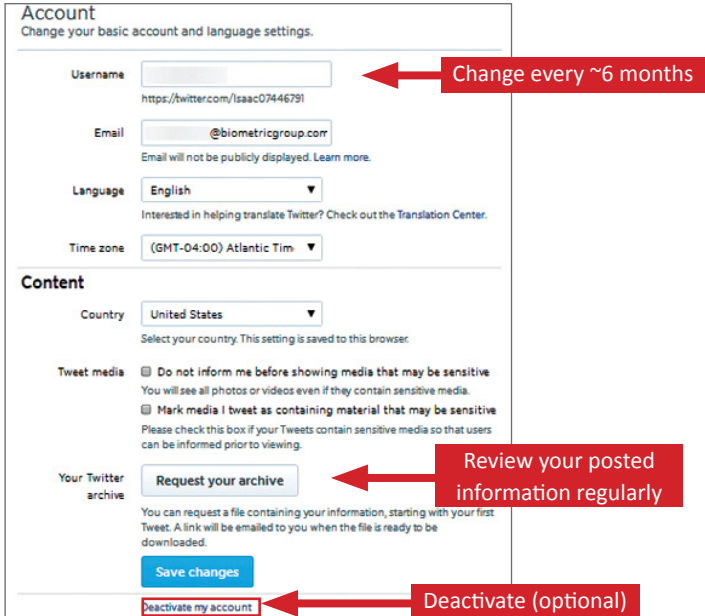


Twitter Best Practices

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

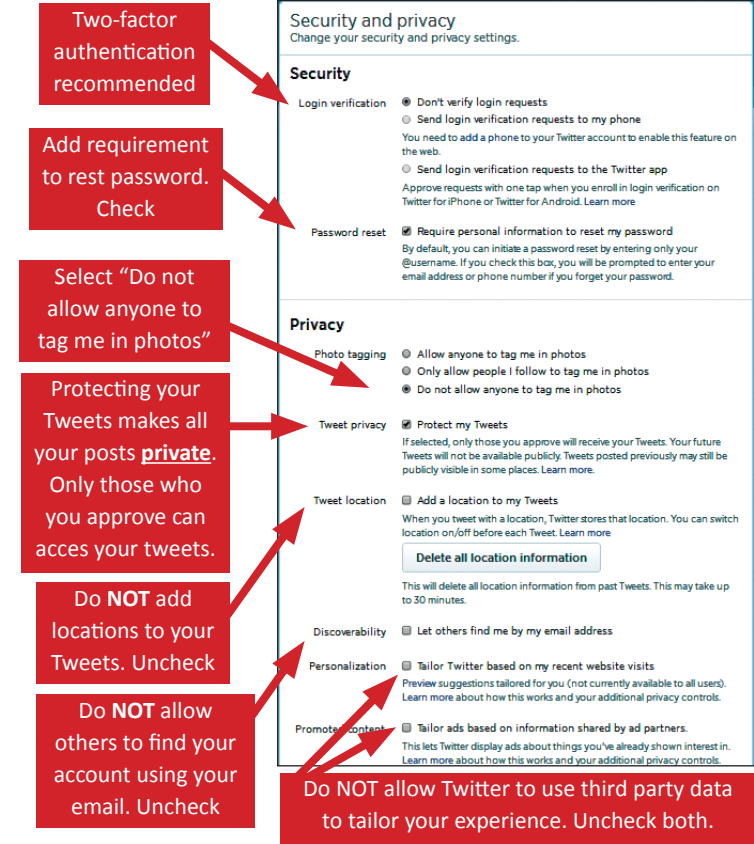
Account Settings

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



Security & Privacy Settings

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



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**.

Two-factor authentication recommended

Add requirement to rest password. Check

Select “Do not allow anyone to tag me in photos”

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

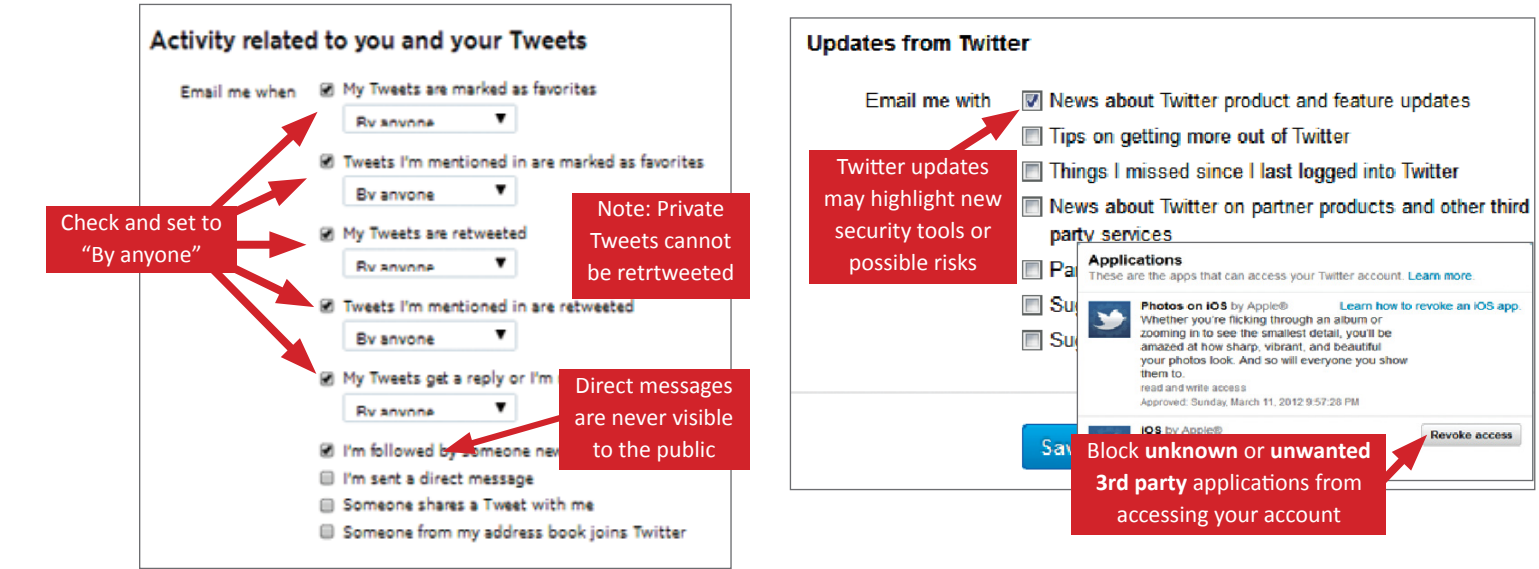
Do NOT add locations to your Tweets. Uncheck

Do NOT allow others to find your account using your email. Uncheck

Do NOT allow Twitter to use third party data to tailor your experience. Uncheck both.

Notification & Application Settings

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



Check and set to “By anyone”

Note: Private Tweets cannot be retweeted

Direct messages are never visible to the public

Twitter updates may highlight new security tools or possible risks

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