



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 **2**

Control how you connect with people you know.

How Tags Work **3**

Control what happens when friends tag you or your content.

Apps and Websites **4**

Control what gets shared with apps, games and websites.

Limit the Audience for Past Posts

Limit the audience for posts you shared with more than friends.

Block Lists

Manage your lists of blocked people and apps.

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: Yahoo! August 22. 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 can bring with them. Uncheck ALL Boxes

Instant personalization: Lets you see relevant information about you arrive on select partner websites. Disable Personalization

Public search: Show a preview of your Facebook profile using a search engine. 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.

Bio My videos

Birthday My links

Family and relationships My notes

Interested in Photos and videos I'm tagged in

Religious and political views Hometown

My website Current city

If I'm online Education and work

My status updates Activities, interests, things I like

My photos 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



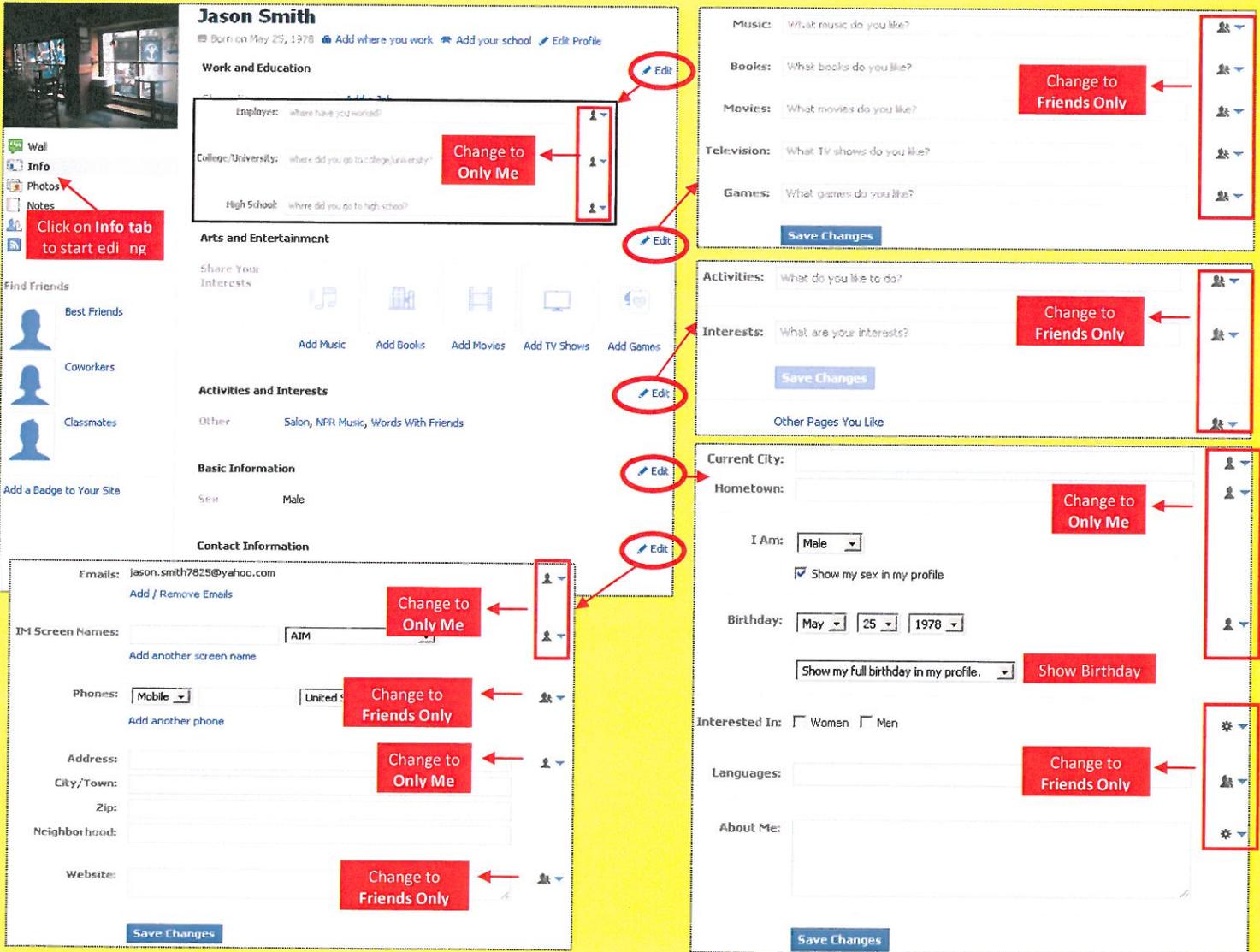
Facebook Smart Card

FB 121211_1800

 Do not login to or link third-party sites (e.g. twitter, bing) using your Facebook account. "Facebook Connect" shares your information, and your friends' information, with third party sites that may aggregate and misuse personal information. Also, use as few apps as possible. Apps such as Farmville access and share your personal data.

Profile Settings

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



Deactivating / Deleting Your Facebook Account



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

To **delete your Facebook account**, go to **Help Center** from the account menu. Type **Delete** into the search box. Select **How do I permanently delete my account** then scroll down to submit your request here. Verify that you want to delete your account. Click **Submit**. FB will remove your data after 14 days post security check.

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



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: **Your circles**
- Who can send you notifications?: **Your circles**
- Who can comment on your public posts?: **Your circles**
- Who can start a Messenger conversation with you?: **Circles**
- Notification delivery:
 - Email: itshelen@gmail.com
 - Phone: **Don't Add Phone Number**
 - Manage email subscriptions: **Uncheck**

- 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

Receive notifications Check as indicated

Notify me by email or SMS when someone... Check as indicated

Posts and mentions of my name

Mentions me in a post	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shares a post with me directly	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a post I created	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a post after I comment on it	<input type="checkbox"/>	<input type="checkbox"/>

Circles

Adds me to a circle	<input type="checkbox"/>	<input type="checkbox"/>
---------------------	--------------------------	--------------------------

Photos

Tags me in a photo	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Tags one of my photos	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Comments on a photo after I comment on it	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a photo I am tagged in	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a photo I tagged	<input type="checkbox"/>	<input type="checkbox"/>

Messenger

Starts a conversation with me	<input type="checkbox"/>	<input checked="" type="checkbox"/>
-------------------------------	--------------------------	-------------------------------------

Google +1

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

Google+ Pages

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

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

Connected accounts

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

Twitter: **Do not add outside accounts**

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

Services

- Delete profile and Google+ features
- Delete entire Google account
- View, enable, or disable 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 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 +300 million active users as of 2011, generating 300 million tweets and 1.6 billion search queries daily.

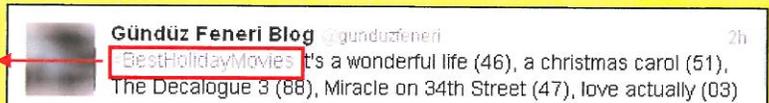


Following are people you subscribe to
Followers subscribe to your tweets
Private tweets will only be visible to followers you approve

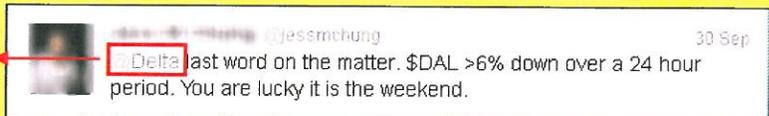
Tweets

"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).

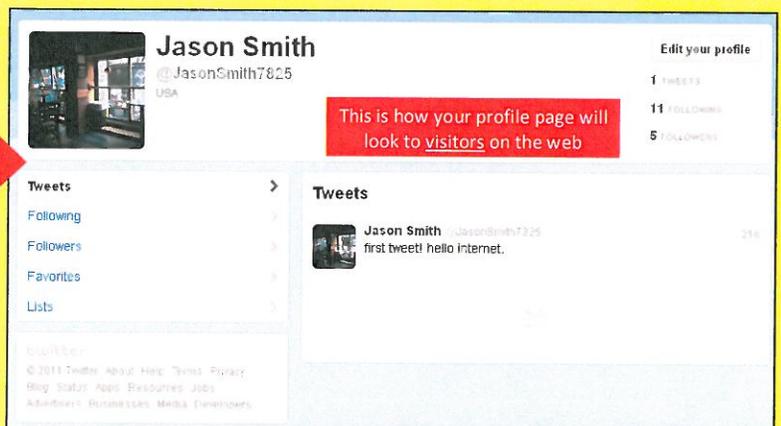
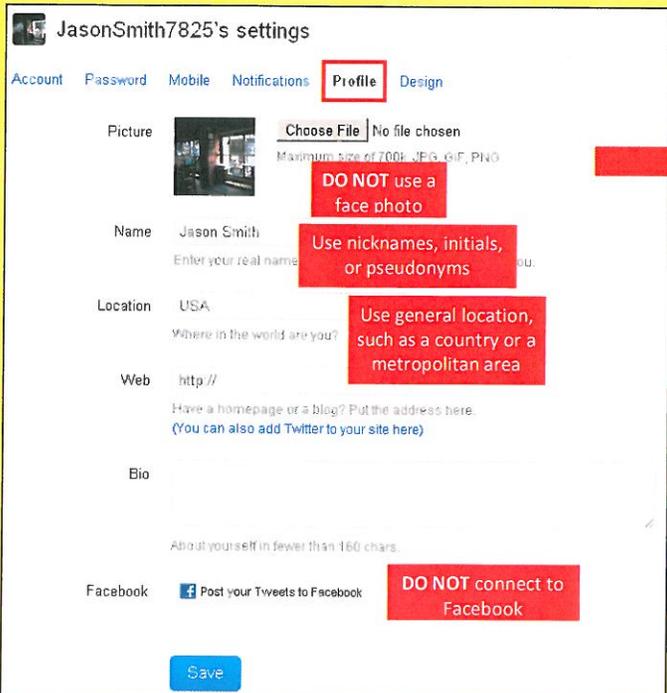


Mentions (@username) are used to tag a user in a Twitter update. When a public user mentions a private Twitter account, the link to the private account profile becomes public.



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** periodically to limit account exposure.



Account Settings

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

JasonSmith7825's settings

Account Password Mobile Notifications Profile Design

DO NOT connect your phone

Name: Jason Smith
You can change your name on your [profile settings](#).

Username: JasonSmith7825
Your public profile: <http://twitter.com/JasonSmith7825>
Change every ~6 months

Email: jason.smith7825@yahoo.com
Note: email will not be publicly displayed
Uncheck Let others find me by my email address

Language: English
What language would you like to Twitter in?
Interested in helping translate Twitter? Check out the [Translation Center](#)

Time Zone: (GMT-06:00) Central Time (US & Canada)

Tweet Location: Add a location to your Tweets
Uncheck
Ever had something you wanted to share ("fireworks", "party", "ice cream truck", or "quicksand...") that would be better with a location? By turning on this feature, you can include location information like neighborhood, town, or exact point when you tweet.
When you tweet with a location, you can turn it on/off before each Tweet.
Click to delete all location data associated with your account
You may **delete all location information** from your 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
Only let people whom I approve to view my Tweets see my Tweets. If this is checked, your future Tweets previously may still be publicly visible. **Protecting your tweets makes all your posts private. Only those who you approve can access your tweets.**

HTTPS Only Always use HTTPS
Use a secure connection where possible to encrypt your account information.

Deactivate my account

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.

Accept **Decline**

Deactivating / Deleting Your Twitter Account

To deactivate your account, go to **Settings** and select **Account** page. 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.

Notifications Account Password Mobile Profile Design Applications

Choose when and how often Twitter sends emails to [itsshelen@gmail.com](#) (change).

Messages

Email me when: I'm sent a direct message **Direct message (DM) is never visible to the public**
 I'm sent a reply or mentioned

Activity

Email me when: I'm followed by someone new
 My Tweets are marked as favorites
 My Tweets are retweeted **Private tweets will become visible to the web when retweeted (RT) by a user with public account**

Updates

Email me with: Occasional updates about new Twitter products, features, and tips
 Product or service updates related to my Twitter account

Save

Applications Account Password Mobile Notifications Profile Design

You've allowed the following applications to access your account

	HootSuite by HootSuite The social media dashboard which allows teams to broadcast, monitor and track results. read, write, and direct messages access - Approved: Tue December 6, 2011 07:18:35 PM	Revoke Access
	Twitter for Android by Twitter, Inc. Twitter for Android read, write, and direct messages access - Approved: Sat February 26, 2011 07:16:46 PM	Revoke Access
	Samsung Mobile by Samsung Samsung mobile own applications read, write, and direct messages access - Approved: Thu February 10, 2011 12:15:07 AM	Revoke Access

Block unknown or unwanted applications from accessing your account

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 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, special interests, 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 with arrows below to ensure that your information is visible only to people of your choosing.

PRIVACY CONTROLS

- Turn on/off your activity broadcasts
- Select who can see your activity feed
- Select what others see when you've viewed their profile
- Select who can see your connections
- Change your profile photo & visibility
- Show/hide "Viewers of this profile also viewed" box

SETTINGS

- Manage your Twitter settings
- HELPFUL LINKS**
- Edit your name, location & industry
- Edit your profile
- Edit your public profile
- Manage your recommendations

Customize Your Public Profile

Control how you appear when people search for you on Google, Yahoo!, Bing, etc.

Profile Content Set to no one

- Make my public profile visible to **no one**
- Make my public profile visible to **everyone**

Basics
Name, industry, location, number of recommendations

Picture

Headline

Current Positions

Interested In...

What others see when you've viewed their profile

- Your name and headline (Recommended)
- Anonymous profile characteristics such as industry and title
Note: Selecting this option will disable Profile Stats.
- You will be totally anonymous.
Note: Selecting this option will disable Profile Stats.

Set to totally anonymous

Who can see your activity feed

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

Only you Set to Only you

Save changes or Cancel

Who can see your connections

Select who can see your connections. Note: People will always be able to see shared connections.

Only you Set to Only you

Save changes or Cancel

Viewers of this profile also viewed...

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

Uncheck

Save changes or Cancel

Upload a Photo

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

Choose File No file chosen

Upload Photo or Cancel

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

- My Connections Set to My Connections
- My Network
- Everyone

Save Settings

Do not use a face photo for your account

LinkedIn Quick Facts

- There are over **100 million** LinkedIn users around the world. Aside from the US, LinkedIn is widely adopted in India, Brazil, and the UK.

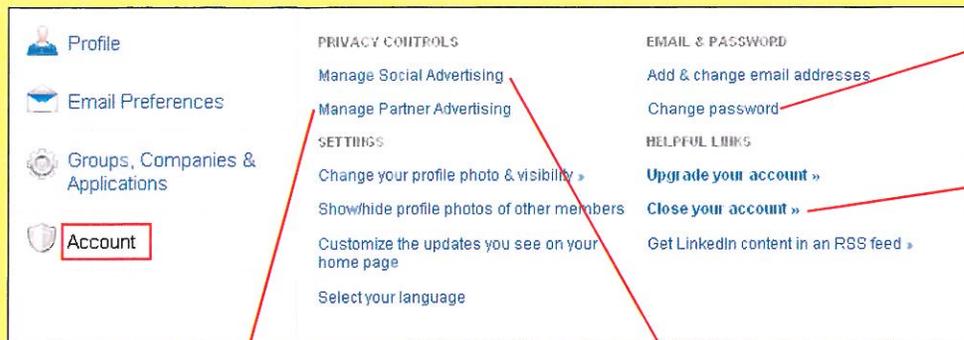
- Users tend to share information related to their **careers or jobs** as opposed to photographs from parties or social events.
- LinkedIn profiles tend to be more **visible and searchable** than in social networks such as Facebook.
- **Paid LinkedIn accounts** have access to more information about other users, such as connections, than free accounts.
- The type of information users can see about each other depends on how **closely they are connected** (1st, 2nd, or 3rd degree).





Account Settings

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

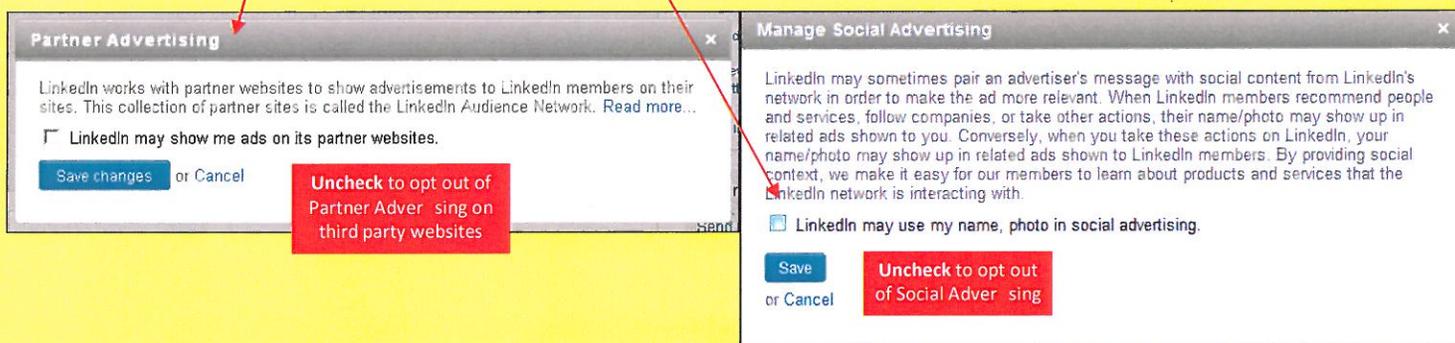


Passwords

Use a complex password with capital letters and numbers to ensure that attackers cannot access your account information.

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.



Application Settings

Third-party applications and services can access most of your personal information once you grant them permission. You should limit your use of applications to ensure that third parties cannot collect, share, or misuse your personal information. Apply the Application setting shown with arrows below to ensure that your information is visible only to people of your choosing.



Also, avoid using the LinkedIn smartphone app to prevent accidentally collecting and sharing location data.



LinkedIn, by default, automatically retrieves information about the user on websites with LinkedIn Plug-In integration. Prevent sharing your activities on third-party websites with LinkedIn by unchecking the box.

Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Wired Kids	www.wiredkids.org/
Microsoft Safety & Security	www.microsoft.com/security/online-privacy/social-networking.aspx
OnGuard Online	www.onguardonline.gov/topics/social-networking-sites.aspx

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!**