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.

1. Change to “Friends Only”
2. How You Connect
3. How Tags Work
4. Choose Your Privacy Settings
5. Info accessible through your friends
6. Limit The Audience for Old Posts on your Profile

[Diagram and instructions for adjusting privacy settings]
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.

![Profile Settings Diagram]

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

- OnGuard Online: [www.onguardonline.gov/topics/social-networking-sites.aspx](http://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 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.

![Google+ Profile Settings](image)
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 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
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
  - Add 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
  - Start a conversation with me

Delete Your Google+ Profile Information or Account

- 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+

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.

**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.

### Deactivating / Delete Your Twitter Account

To deactivate your account, go to **Settings** and select **Account** page. At the bottom of the page, click "**Deactive 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.

**Useful Links**

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

**Useful Links**

- [www.wiredkids.org/](http://www.wiredkids.org/)
- [www.microsoft.com/security/online-privacy/social-networking.aspx](http://www.microsoft.com/security/online-privacy/social-networking.aspx)
- [www.onguardonline.gov/topics/social-networking-sites.aspx](http://www.onguardonline.gov/topics/social-networking-sites.aspx)
LinkedIn Smart Card

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

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).
LinkedIn Smart Card

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

Wired Kids  www.wiredkids.org/
OnGuard Online  www.onguardonline.gov/topics/social-networking-sites.aspx