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.
- 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.

Managing Your LinkedIn Profile

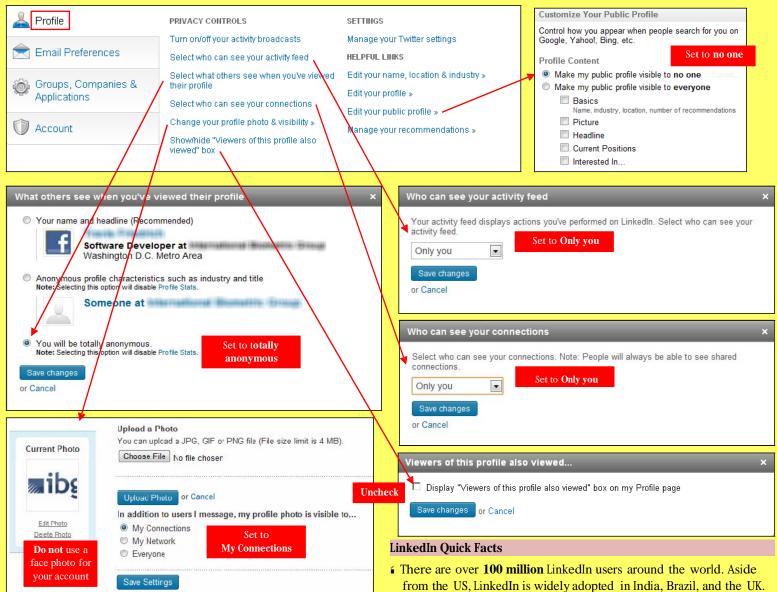
LinkedIn is a professional networking site whose users establish connections with co-workers, customers, business contacts, and potential employees and employers. Users post and share information about current and previous employment, education, military activities,



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.

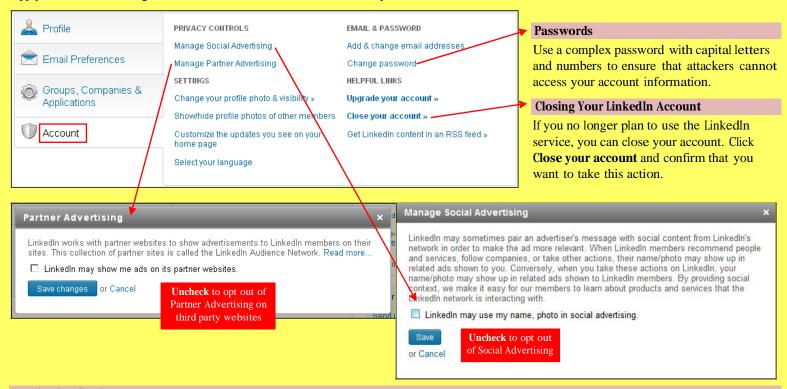


- Users tend to share information related to their careers or jobs as opposed to photographs from parties or social events.
- LinkedIn profiles tend to be more **visible and searchable** than in social networks such as Facebook.
- Paid LinkedIn accounts have access to more information about other users, 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).



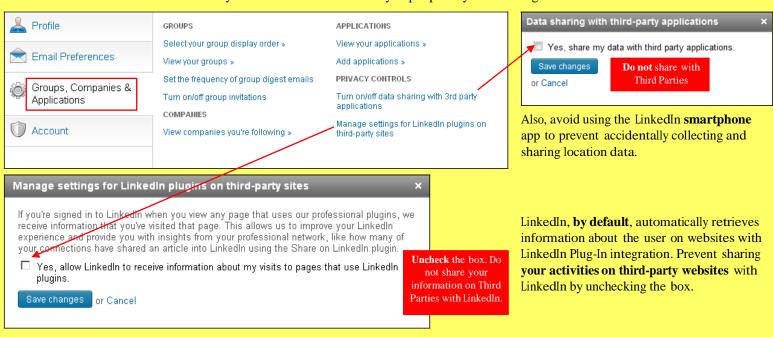
Account Settings

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



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.



Useful Links

A Parent's Guide to Internet Safety
Wired Kids
Wired Kids
Www.wiredkids.org/
Microsoft Safety & Security

OnGuard Online

www.microsoft.com/security/online-privacy/social-networking.aspx

www.onguardonline.gov/topics/social-networking-sites.aspx