# 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.

Use **Settings** to manage visibility
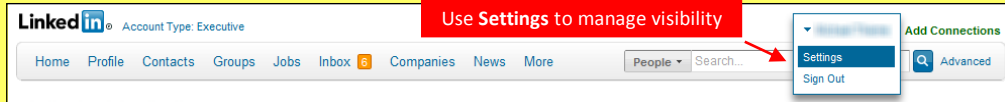
Profile Settings

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

Set to **no one**

Set to **Only you**

Set to **Only you**

Uncheck

Set to **totally anonymous**

Set to **My Connections**

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.

Uncheck to opt out of Partner Advertising on third party websites

Uncheck to opt out of Social Advertising

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.

Do not share with Third Parties

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

Uncheck the box. Do not share your information on Third Parties with LinkedIn.

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