

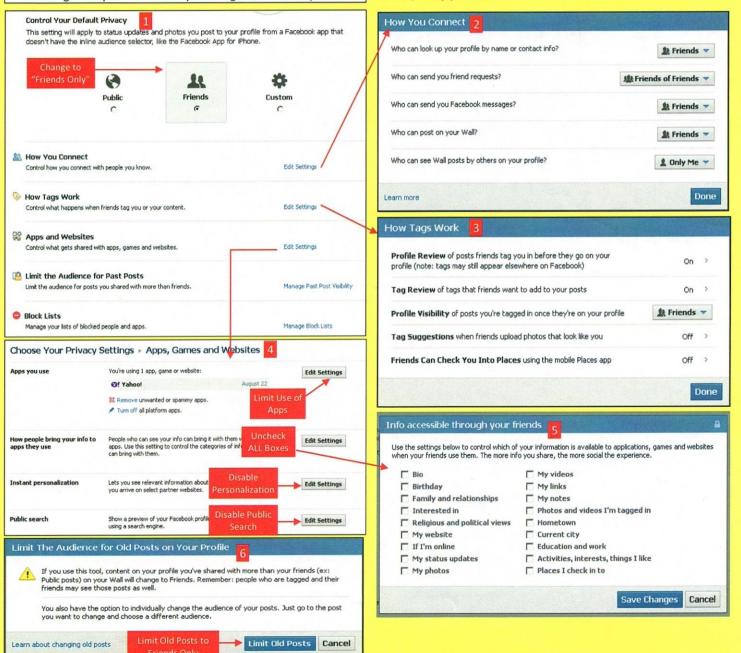
# **Facebook Smart Card**

#### 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.



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.





# **Facebook Smart Card**



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** 

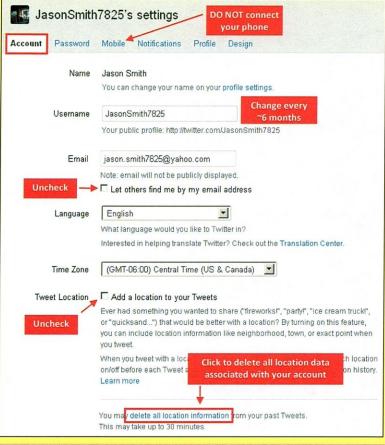
www.fbi.gov/stats-services/publications/parent-guide www.wiredkids.org/

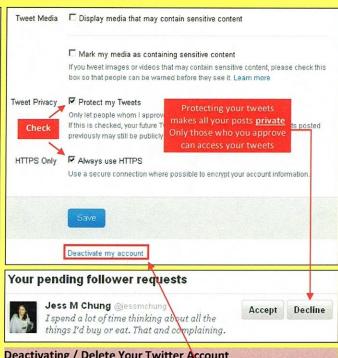


# **Twitter Smart Card**

### **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 deactive 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

www.fbi.gov/stats-services/publications/parent-guide

www.wiredkids.org/

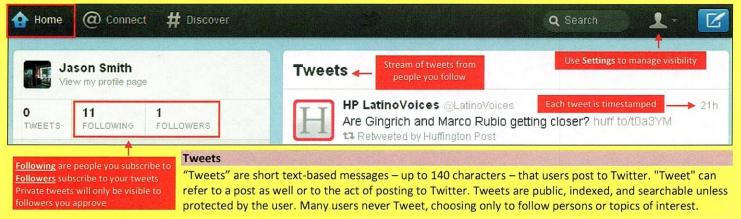


## Social Networks -Do's and Don'ts

- · 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.



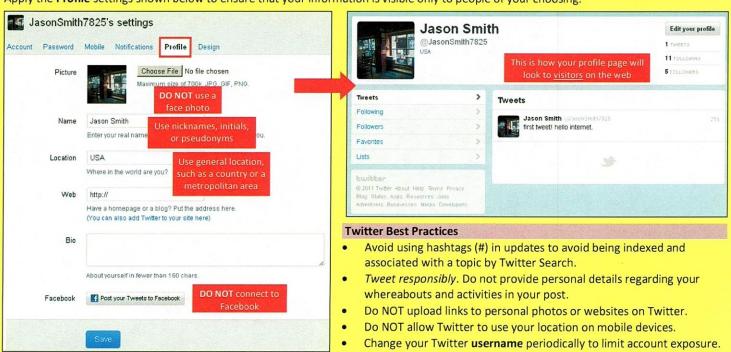
**Hashtags (#topic)** are used to mark a keyword or topic in a Tweet. Posts with hashtag are categorized by topics in the Twitter search engine. Hashtagged words that become popular become Trending Topics (ex. #jan25, #egypt, #sxsw).

**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.





# 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**

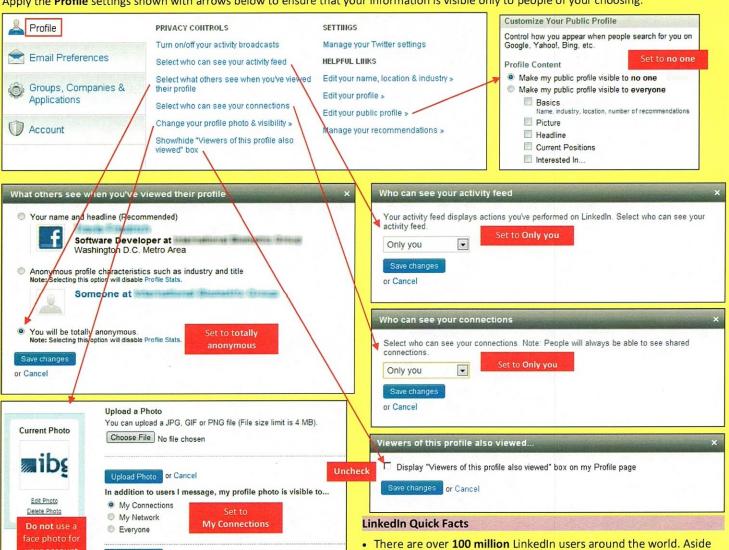
LinkedIn is a professional networking site whose users establish connections with co-workers, customers, business contacts, and potential employees and employees. Users post and share information about current and previous employment, education, military activities,



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 (1<sup>st</sup>, 2<sup>nd</sup>, or 3<sup>rd</sup> degree).

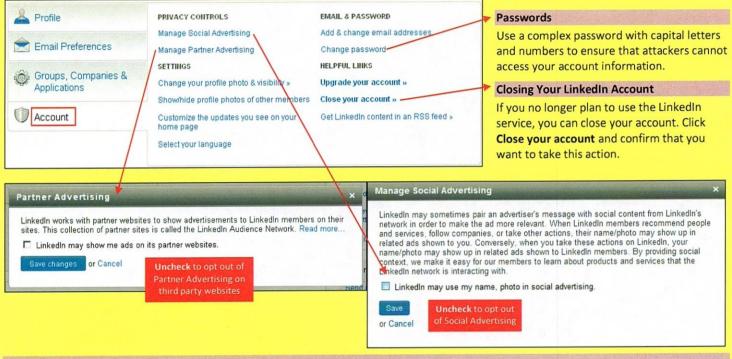


from the US, LinkedIn is widely adopted in India, Brazil, and the UK.



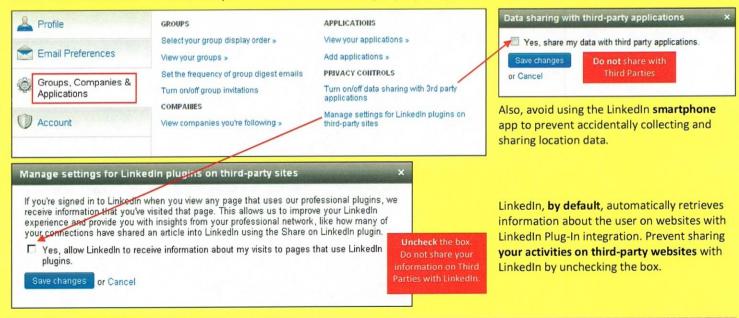
### **Account Settings**

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



## **Application Settings**

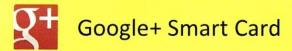
Third-party applications and services can access most of your personal information once you grant them permission. You should limit your use of applications to ensure that third parties cannot collect, share, or misuse your personal information. Apply the **Application** setting shown with arrows below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



## **Useful Links**

A Parent's Guide to Internet Safety Wired Kids Microsoft Safety & Security OnGuard Online www.fbi.gov/stats-services/publications/parent-guide

www.wiredkids.org/



### 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.

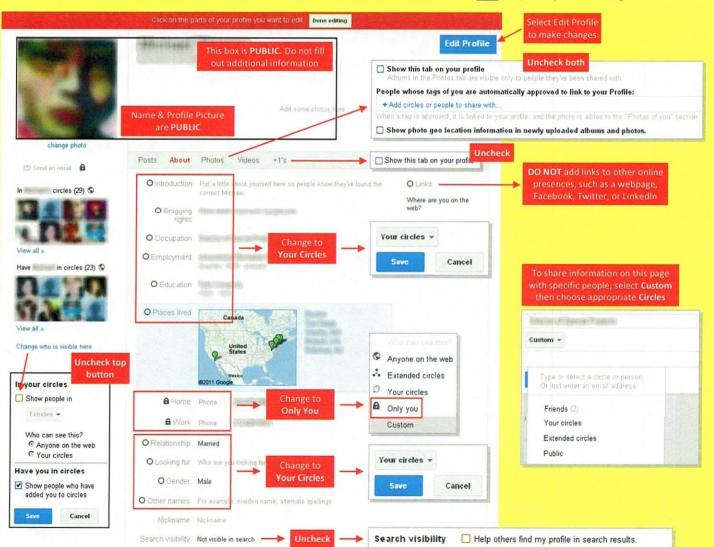
#### Managing Your Google+ Profile

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**

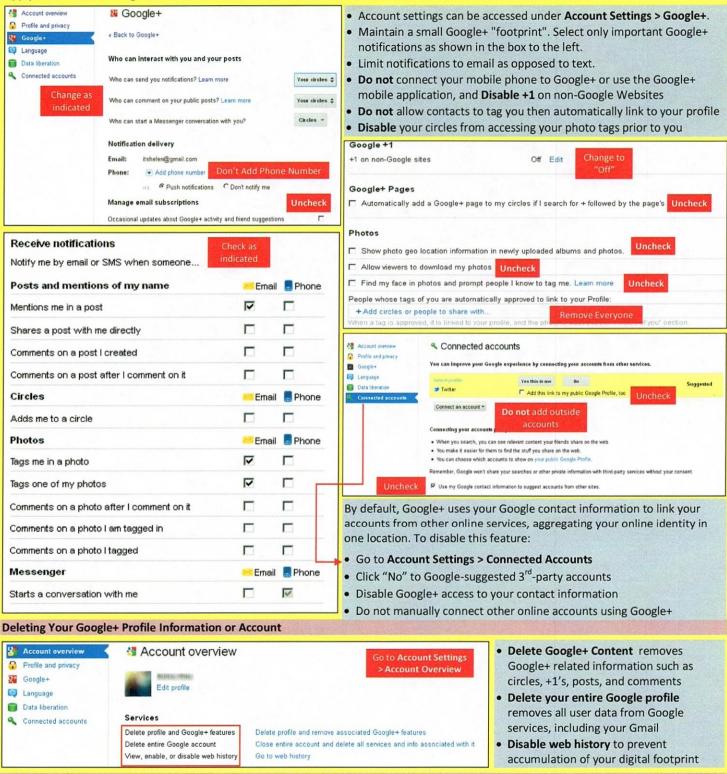
Apply and save the Profile settings shown below to ensure that your information is visible to only people of your choosing.





### **Account Settings & Minimizing Your Activities**

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



## **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/