Facebook Mobile Overview

As of January 2015, Facebook Mobile hosts 745 million daily mobile active users who accounts for over 60% of all mobile posts published to any online social networking service. Though privacy can still be achieved, mobile users place their personal identity data at a greater risk when compared to users logging in via desktop computer. This is in large part due to the fact that mobile devices provide Facebook with a means to access additional location information, contact lists, photos, and other forms of personal data. Use the following recommendations to best protect yourself against oversharing.

Facebook Mobile Settings

Facebook Mobile’s general security settings closely resemble those of Facebook’s desktop application. Click More on the Facebook banner and select Settings. From there, navigate through the Security, Privacy, Timeline and Tagging, and Locations tabs to apply the settings shown below.

Review active sessions and devices to spot unauthorized activity

Your Active Sessions

Current Session
Location: Washington, DC, US
Device Type: Facebook for iOS on iOS 7
Device Name: Facebook for iPhone

If you see an unfamiliar device or location, remove it to end its session.

Your Recognized Devices

This device:
Facebook for iPhone
September 4, 2013

Other devices:
Chrome on Windows
January 25, 2014

Review all added content

Disable Location History to prevent Facebook from logging your precise location at all times

iPhone Settings

The iPhone’s security settings can help to further protect your personal data while you use the Facebook Mobile App. From the iPhone’s Settings icon, select Privacy and navigate through the Location Services, Photos, and Facebook tabs to disable all of the permissions, as seen below.

Android Settings

Android phones can be configured to protect your personal data while you access the Facebook Mobile App. Access the phone’s general Settings feature and navigate through the Location Access and Apps tabs to limit the amount of data that Facebook can take from your device.

Review the permissions Facebook requires access to once the mobile app is downloaded

Social Network - 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.
### Posting to Facebook

**Update Status**

- **To:** Friends
- *What's on your mind?*

**Share With**

- **Only These Friends**
- **Friends except...**
- **More...**

**Add Photos**

- Add Location

**Tag Friends**

- Tag Friends
- *What Are You Doing?*

**What Are You Doing?**

- Feeling
- Watching
- Reading

**Add Location**

- Add Location

---

**Nearby Friends**

- **Nearby Friends** is a feature that allows you to share your location with friends. When activated, this feature routinely broadcasts your approximate location to your friends. You also have the option to allow certain users to see your precise location for set periods of time.

**Nearby Places**

- **Nearby Places** is a feature that uses your GPS location to display local venues. When activated, the feature displays the distance to and ratings from other users about the destination. When a venue is selected, individual reviews appear with links to the posters' profiles. Don’t post on these public threads.

**Useful Links**

- A Parent’s Guide to Internet Safety
- Privacy Rights Clearinghouse
- Microsoft Safety and Security
- Online Guardian

- [www.privacyrights.org/fs/fs18-cyb.htm](http://www.privacyrights.org/fs/fs18-cyb.htm)
- [www.microsoft.com/security/online-privacy/social-network](http://www.microsoft.com/security/online-privacy/social-network)
- [www.onguardonline.gov/topics/social-networking-sites.aspx](http://www.onguardonline.gov/topics/social-networking-sites.aspx)