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.

Minimizing Your Facebook Profile

Facebook provides shortcuts to their privacy settings that help to limit what others can see in your profile. Select Privacy Checkup to change your basic privacy settings. For more extensive settings, click See More Settings. From there, navigate through the pages of the settings toolbar to control how your personal information is shared with others.

1. Use the Privacy tab to declare which audiences can search for you, contact you, and see your posts. In general, it is best to limit the audiences to ‘Friends’ or “Only Me”. The Use Activity Log selection can be used to review past posts individually and edit the audiences for each entry. The Limit Past Posts selection can be used to retroactively change the settings of all ‘Public’ posts to a ‘Friends’ only audience.

2. Timeline and Tagging controls how others interact with your timeline. Select View As to see what your profile looks like to specific audiences.

3. Followers can view your posts from their personal News Feeds. It is even possible for followers to view the content you post without being an accepted Facebook friend. Set Who Can Follow Me to ‘Friends’ only.

4. The Security tab provides ways to protect your credentials and become aware of suspicious login attempts. Use Login Alerts and Where You’re Logged In to monitor login activities and end inactive sessions.

5. Use the Ads tab to prevent Facebook from using your data for advertising. Set Third Party Sites and Ads & Friends fields to ‘No One’.

6. Your Facebook contacts may be sharing your information with third party apps without your knowledge. Navigate Apps > Apps Others Use and uncheck all data fields to prevent others from sharing your data.

Facebook Smart Card

Minimizing Your Facebook Profile

1. Use the Privacy tab to declare which audiences can search for you, contact you, and see your posts. In general, it is best to limit the audiences to ‘Friends’ or “Only Me”. The Use Activity Log selection can be used to review past posts individually and edit the audiences for each entry. The Limit Past Posts selection can be used to retroactively change the settings of all ‘Public’ posts to a ‘Friends’ only audience.

2. Timeline and Tagging controls how others interact with your timeline. Select View As to see what your profile looks like to specific audiences.

3. Followers can view your posts from their personal News Feeds. It is even possible for followers to view the content you post without being an accepted Facebook friend. Set Who Can Follow Me to ‘Friends’ only.

The Security tab provides ways to protect your credentials and become aware of suspicious login attempts. Use Login Alerts and Where You’re Logged In to monitor login activities and end inactive sessions.

Remember, Facebook interactions such as likes and wall posts have been effectively used to profile individuals based on their behaviors. Try to minimize the amount of personal information that you post on social networking services and limit your interactions.

Avoid linking third-party apps (e.g. Twitter) with your Facebook account. Data shared with other apps becomes subject to their terms and conditions which may result in unwanted data aggregation and dissemination.
Facebook Profile Page

The Facebook profile page contains tabs that allow users to add information about themselves, view friend lists, and post text entries or photos to their profiles. Within these tabs reside general audience settings. Use the guidelines below to maximize your security while interacting with these features.

About

Avoid entering personal data within the About section. This information is mostly optional and contains data fields including Work and Education, Places You’ve Lived, Contact and Basic Info, Family and Relationships, and Details About You. Use the audience settings to change the mandatory fields to ‘Friends’ or ‘Only Me’.

Friends

Under the Friends tab:

- Navigate Manage > Edit Privacy to change who can view your contacts. Limit your Friend List to Only Me.
- Navigate Manage > Manage Sections to control which data fields will appear on your timeline. Avoid sharing places on your timeline and use discretion when posting information regarding your personal interests.

View Activity Log

The View Activity Log tool displays the information that is posted to your timeline in a chronological order. Use the dropdown menu shown to delete or manage how individual posts appear on your timeline.

Deactivating/Deleting Your Facebook Account

Deactivating an account removes your name and photos from things that you have shared. To deactivate your Facebook account, navigate to Settings > Security > Deactivate Your Account. Your account remains deactivated until the next time you login.

To delete your Facebook account, select Help from the triangle icon’s dropdown menu and select Visit the Help Center. Navigate Manage Your Account > Deactivating, Deleting & Memorializing Accounts > How do I Permanently Delete My Account > Let Us Know. Verify that you wish to delete your account by clicking Delete My Account. Facebook will permanently remove most of your data within 90 days of submission.

Useful Links - For more information or questions regarding this card email smartcards@novetta.com

Privacy Rights Clearinghouse www.privacyrights.org/fs/fs18-cyb.htm
Microsoft Safety and Security www.microsoft.com/security/online-privacy/social-network
Online Guardian www.onguardonline.gov/topics/social-networking-sites.aspx