Social Media Roundup

9 Critical Steps: Protecting Yourself on Facebook
Social Media Roundup

Agenda

This week’s Social Media Roundup outlines 9 critical steps that can help protect your personal information and privacy while on Facebook.

- Introduction
- 9 Critical Steps
- Additional Resources
Social Media Roundup

Introduction

- Facebook is an effective tool Army organization members can use to communicate their messages and tell organization stories. Facebook is also a way for Soldiers to stay connected. But Facebook use is not without its risks.
- Sharing too much information on Facebook can result in OPSEC violations, identity theft, spam, home break-ins and computer viruses.
- Using social media platforms like Facebook should be a balance between communicating with friends and family and protecting your privacy and online safety.
- Facebook’s default privacy settings are often public, but Facebook provides various setting options that help Facebook users adjust and customize their privacy settings.
9 Critical Steps

#1: Friends Only
#2: Less Sharing
#3: Personal Protection
#4: App Remover
#5: Limited Access
#6: Don’t Take it Personal
#7: Stealth Mode
#8: Good Networking
#9: Don’t Become a Target
Step #1: Friends Only

- To take a closer look at your settings, click on your account at the upper right corner of your page. As you’ll see, if you haven’t already adjusted them, your privacy settings will be set to the Facebook default.
Social Media Roundup

Friends Only

- These are the settings recommended by the Army. Sharing only with friends eliminates the risk of your content falling into the hands of people you’ve never met.
- When you list something as “other” it typically means you’ve customized your settings further than the categories offered in the first three columns.
Step #2: Less sharing

- After changing the basic sharing settings, click on the “customize settings” link at the bottom of the page. This will allow you to further customize what you share with others.
Once you’ve clicked through to the “customize settings” link, the Army recommends you change your settings to match the screenshot below.

<table>
<thead>
<tr>
<th>Things I share</th>
<th>Posts by me</th>
<th>Family</th>
<th>Relationships</th>
<th>Interested in and looking for</th>
<th>Bio and favorite quotations</th>
<th>Website</th>
<th>Religious and political views</th>
<th>Birthday</th>
<th>Places I check in to</th>
<th>Include me in &quot;People Here Now&quot; after I check in</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default setting for posts, including status updates and photos</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Visible to friends and people checked in nearby. (See an example)</td>
</tr>
<tr>
<td></td>
<td>Friends Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Enable</td>
</tr>
</tbody>
</table>
Step #3: Personal Protection

- Once you change your sharing settings, take a look at the other setting options. Click on “view settings” at the top.
- This takes you to a page where you can control your privacy settings even further.
- Once you click through, you’ll be able to adjust how you can be searched and who can view your basic information.

Choose Your Privacy Settings

- Connecting on Facebook: Control basic information your friends will use to find you on Facebook. View Settings
- Sharing on Facebook: These settings control who can see what you share.

<table>
<thead>
<tr>
<th>Everyone</th>
<th>Everyone</th>
<th>Friends of Friends</th>
<th>Friends Only</th>
</tr>
</thead>
</table>
Once on this page, the Army recommends changing all of the default settings to match those on the right.
Personal Protection

- Continue moving down the page and make changes to what others can share on your page and who can view your contact information. Follow the suggested settings on the right.
Step #4: App Remover

- Next, go back to your settings page and click on the “Apps and Websites” link at the bottom of the page.
- By default, apps have access to your friends list and any information you choose to share with everyone.
- This page allows you to delete apps you do not trust.
App Remover

- Make sure you remove any unwanted applications and make your game and application activity visible to friends only.
Step #5: Limited Access

- Make sure you also click on “info accessible through your friends”.

![Diagram showing steps](image)
Limited Access

- Then unselect everything and save your changes.
- Reminder: This is the information applications access through your friends, so be careful what you leave checked.
Step #6: Don’t Take it Personal

- Next, edit your settings in the “Instant personalization” option.
Don’t Take it Personal

- Uncheck the box that reads “enable instant personalization on partner websites”. This will keep Facebook’s partner companies from accessing your personal information.
Step #7: Stealth Mode

- The last stop on this page is the “public search” option.
Stealth Mode

- It is recommended that you uncheck the “enable public search” box.
- This will keep your profile from appearing when people search for your name.
- If you leave public search enabled, content you share with “Everyone” is open to anyone on the web, not just Facebook.
- Once you unchecked this function, it will take a short period of time for the change to register and for your profile to stop appearing in searches.
Step #8: Good Networking

- Networks help you stay in touch with old friends, and help you reconnect with people you’ve lost touch with, but belonging to a network can also be dangerous if you’re not careful.
- By opening your information up to a network, you may share information with people you do not know.
- To change your network, go to “Account Settings” then select the “Networks” tab. Select “Leave Network” to remove that network, or type in your workplace or school to search for networks to join.
Step #9: Don’t Become a Target

- Facebook can use your information to target advertisements toward your friends.
- Unless you want Facebook to have unique access to your friends and family on Facebook, it’s advised that you disable this function.
- You can do this by clicking on “account settings,” and selecting the Facebook Ads Tab. Then select the “No one” option for allowing ads from third party applications. Then select the “No one” option for showing my social actions in Facebook Ads.
Summary

- Facebook is an effective tool Army organization members can use to communicate their messages and tell organization stories. Facebook is also a way for Soldiers to stay connected. But Facebook use is not without its risks. Sharing too much information on Facebook can result in OPSEC violations, identity theft, spam, home break-ins and computer viruses.

- Facebook's default privacy settings often leave much of your private information public, so it's important to take a closer look at your privacy settings and see how you can better protect yourself.

- It's up to the individual users to adjust their settings. If users choose not to adjust their settings, they will operate with the default settings which can put a lot of private information out in the open.

- Adjusting your privacy settings to the Army’s recommended settings will help you better protect yourself and your personal information.
Additional Resources

- Facebook and Privacy Page: http://www.facebook.com/fbprivacy
- Army Social Media Handbook: http://slidesha.re/es9GLr
Contact information

Have questions? Please feel free to reach out to us at the Online and Social Media Division

Email: Ocpa.osmd@us.army.mil

To review and download past editions of the Social Media Roundup, visit our Slideshare site at: http://www.slideshare.net/usarmysocialmedia.

All Social Media Roundups are authorized to be distributed to a broader audience.

2/23/2010

OFFICE OF THE CHIEF OF PUBLIC AFFAIRS
PENTAGON