



SOCIAL MEDIA CHECKLIST

1. MANAGING A MAINE NATIONAL GUARD ASSOCIATED PAGE

- Designate members of your team responsible for posting content to the official on line presence.
- Make sure all content is submitted to, and approved by the commander or the organization's release authority.
- Make sure all content posted is in accordance with organization Public affairs Guidance and Army Regulations. AR 360-1, FM 3-61.
- Monitor your Social Media presence and make sure external social media users are not posting sensitive or offensive information on your official presence. Monitor your social media presences
- Produce training materials and conduct regular social media OPSEC training with your team and with other units of your organization.
- Distribute social media OPSEC training to the families of your Soldiers. It's important to keep them just as informed and up-to-date as the Soldiers of your unit.
- Be Vigilant. Never become complacent when it comes to OPSEC. Check social media presences within your organization for violations. Never stop working to protect OPSEC. Once the information is out there, you can't take it back.
- Guard members should not release personal identifiable information, such as Social Security number, home address or driver's license number that could be used to distinguish their individual identity or that of another Guardsman.

2. TIPS ON SECURITY

- If you are a member of a social network, pay close attention to your privacy settings, which allow you to choose how much personal information you reveal and to whom
- Carefully consider what you publish on social networks. Before you post photos, videos, or text, ask yourself if it would embarrass you if your family or employer saw them.
- Before you add a widget (an application that can be shared with others electronically) to your profile, think about whether you want the creators of the widget to be able to access your profile page and information about your activity on the social network. Keep in mind that the social network generally has no control over these widgets, so exercise discretion when using these tools.
- Report any abuses of a website's Terms of Use to the website's administrators. Any reputable website or social network will have a way for you to report abuse.
- E-mail can be used to spread malicious software or obtain your personal information in order to commit fraud. Never post your personal contact information, to include email or phone number.
- Pictures and postings having multiple aspects of personal data, to include full name, hometown, family members name or other uniquely identifying information should only be posted and shared by the MENG PAO Sites, and can then be shared to lower sites, if desired.

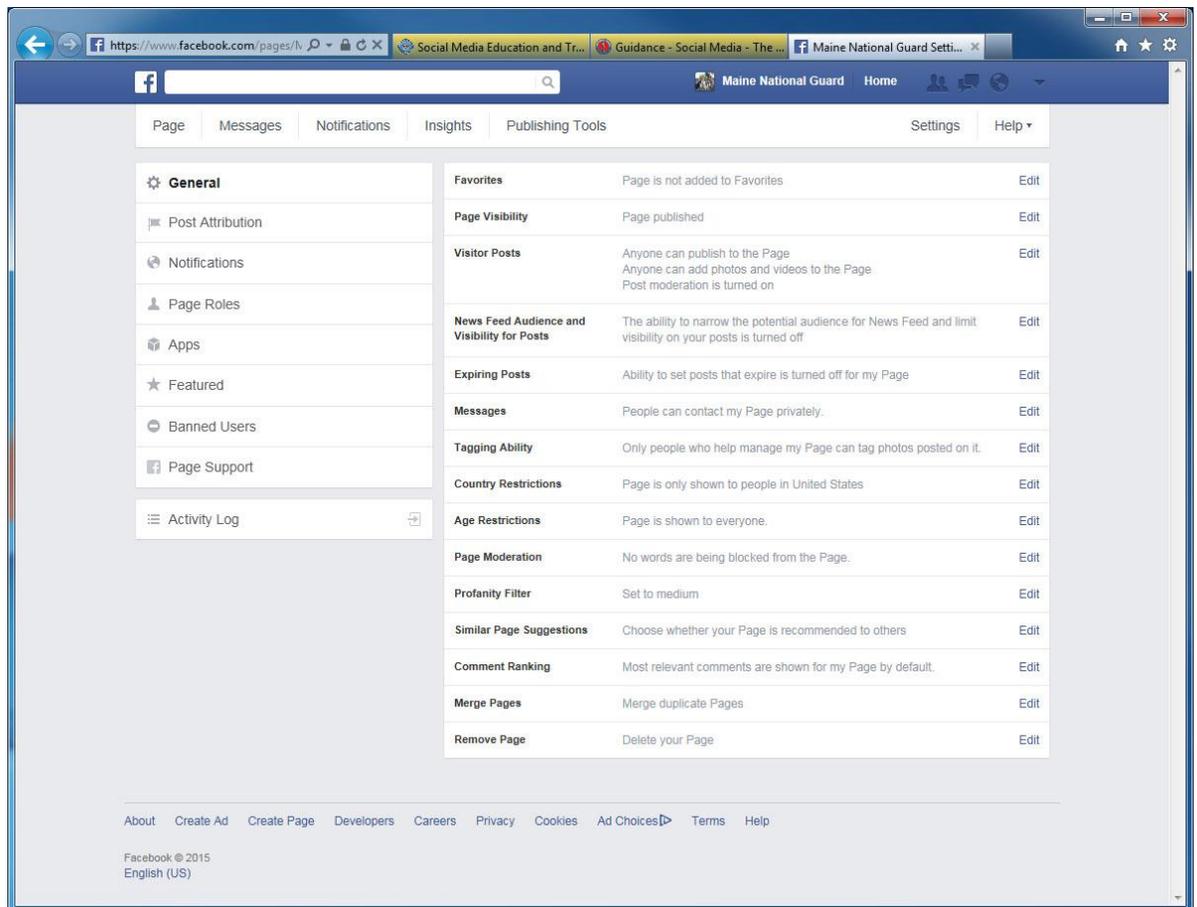
3. TIPS ON SAFTEY

- Guard members should not release personal identifiable information, such as Social Security number, home address or driver's license number that could be used to distinguish their individual identity or that of another Guardsman.

- Guard members are also not allowed to release National Guard email addresses, telephone numbers or fax numbers not already authorized for public release. By piecing together information provided on different websites, criminals can use information to impersonate Guard members and steal passwords.
- Finally, Guard members should review their accounts daily for possible use for changes by unauthorized users and should install and maintain current anti-virus and anti-spyware software on their personal computers.

4. SETTINGS FOR FACEBOOK PAGES APPROVED BY THE PAO & OPSEC OFFICER

- Make SFC Peter Morrison a page administrator
- Ensure admins of the page have conducted DOD Social Media class and OPSEC classes
http://iaseapp.disa.mil/eta/sns_v1/sn/launchPage.htm
- Do not allow tagging of photos, either persons or locations.
- Do not allow unregulated comments. Any and all comments must be approved by a page admin prior to being posted.
- Do not post pictures of civilians or children without proper consent.



Example of proper settings.