PRECAUTIONS FOR THE USE OF
SOCIAL NETWORKING SITES
FOR ANTITERRORISM AWARENESS
AND COMMUNITY OUTREACH

VOLUME II
MAY 2015
Purpose: This guide provides a consolidation of current and relevant precautionary and protective measures designed to mitigate the risk of using social networking sites. The primary sources for information in this guide are recently released official messages from Headquarters Department of the Army and U.S. Northern Command as well as detailed information from the Defense Media Activity and the U.S. Army Criminal Investigation Command’s Cyber Crime Investigation Unit. Citations and websites for source documents are provided throughout to facilitate additional education.

Audience: This guide is intended to assist the antiterrorism officers and Family Readiness Groups at all levels in understanding the risks associated with using social media and the common protective measures to mitigate those risks.
CONTENTS

Introduction—Stay Safe ................................................................................................................. 1
DoD Precautions ............................................................................................................................. 3
Technical Protective Measures ....................................................................................................... 11
Additional Resources ..................................................................................................................... 23
In light of the threats against Soldiers and their Families by terrorist organizations, many DoD organizations to include the Department of the Army have published social media messages and precautions. This guide provides published precautions and recommended practices to help protect our Soldiers and Families.
STAY SAFE WHEN USING SOCIAL MEDIA

Social networking sites and other social media are popular with Army community members, their families, and friends for keeping in touch. These media are also an integral part of individual and organizational communications across the Army and the broader Department of Defense. The role these media play in personal and official communications requires security precautions, described in this guide. Follow these precautions to protect yourself and your family, friends, and fellow Soldiers.

WHAT IS A SOCIAL NETWORKING SITE?

A social networking site, according to the National Security Agency, “is a web-based service that allows communities of people to share common interests and/or experiences. Rather than “stay in touch by meeting face to face or with phone, text, or video messages, social networking sites “allow users to publish information that can be read later by other users (a one-to-many form of communication) and follow their friends’ postings and provide comments.” Many social networking sites “also allow users to logon from mobile devices that have web browser access to the Internet, allowing them to check and update their accounts from virtually any location with a Wi-Fi or cellular signal.”

Associated Risks

Social networking sites “promote ‘social behavior’ and encourage users to share information and inherently trust the information from those they are connected to within the network. “Once information is posted or uploaded onto” a social networking site, “it should no longer be considered private.” In fact, social networking sites can present an operations security risk to military units and a direct risk to the individual: “Cyber attacks [and other risks associated with using social networking sites] are a real and present threat to the cyber security of government social media accounts,” according to the Defense Media Activity.

---

3 Defense Media Activity, “Guide to Keeping Your Social Media Accounts Secure,” 2015
This section provides DoD and Army overarching precautions and recommended practices which can be applied across the entire Army community to help protect our Army communities from the risks associated with using social media. Terrorists and other threat groups are attempting to use our own personal information against us to create fear and anxiety within the military ranks. We all have a responsibility to protect ourselves and others within our military communities. We must reduce our vulnerabilities through active and vigilant monitoring of the information provided via social networking sites and social media.
Think before you post. Always assume everyone in the world will be able to see what you are posting, or tweeting, even if the site limits your posts to your friends and family.

Do not allow others to tag you in images they post. Doing so makes you easier to locate and makes it easier to accurately reconstruct your network of friends, relatives, and associates. You are not anonymous on the Internet.

Be cautious about the images you post. What is in the photos may be more revealing than who is in them. Images posted over time may form a complete mosaic of you and your family.

Once something is posted on a social networking site, it can quickly spread. No amount of effort will erase it.

Review privacy settings and limit who can view your social media sites; but do not trust these settings as absolute.

Avoid posting your home or work address and phone numbers.

Limit any reference to military, government, or law enforcement employment or affiliation, current or former, on social media.

Avoid providing detailed accounts of your day (for example, when you leave for or return from work).

Do not use “check-ins,” which report your location. If they are enabled, disable them.

Never allow applications to geo-locate you.

Do not post personally identifiable information on social media.

Do not arrange meetings with people you meet online.

Do not use your social networking site to login to other sites. Create another user account on the new site instead.

Use strong, unique passwords. Consider using passphrases for an additional level of security.

Keep your antivirus software current.

---

4 Urgent ALARACT Message (055/2015), slightly edited
Physical and Home Security Precautions

While most of these measures are primarily geared toward preventing home burglaries, when implemented these same measures can help protect you and your family:

- Always lock doors, windows, and garages.
- Make sure home entrances are well lighted, and minimize bushes where intruders can hide.
- Use the peephole (or look through a window) before opening the door to anyone. Don’t use the chain latch to open the door part-way.
- Don’t open the door to solicitors or strangers.
Issue Internet and media use smart cards which detail safe online practices.

Reenergize suspicious activity reporting campaigns.

Educate and inform military, civilians, contractors, and family members about potential risks and security measures. Address these topics at community venues (such as town halls, family readiness group meetings, commander’s calls) and/or use print and electronic means (newsletters, newspapers, command announcements and broadcast messages, web page banners) to convey the message.

Highlight the amount of publicly available information about Service members and their families and the potential security vulnerabilities and personal protection concerns posed by social networking sites and further exploitable via the Internet. The use of the Internet and social networking sites by Service members or their family can present unique security concerns that must be understood by all. It is likely that poor operations security and poor protection of personally identifiable information could result in increased security and force protection risks to units, individual Service members, and family members.

Ensure that Service members understand that unintentional disclosure of critical information and personally identifiable information may pose a risk to them, their family, and the Defense Department and Army mission. Advise them of the types of military and personal information that may be exploited and how.

Advise Service members of what information is safe to share or discuss (for example, information that has been released to the public, general locations, and pride in and support for organizations or individuals).

Educate members on how unsolicited contacts, unknown friends, and followers may exploit and elicit them for sensitive personal, financial, and military information.

Develop and distribute (or post) a list of guidelines for social media interaction that address privacy settings and content.

---

5 Adapted from Headquarters, U.S. Northern Command, Force Protection Advisory 15-092, Security Awareness, 2 April 2015
Privacy Settings

Each social media site allows all of your private profile information, as well as your posts, to be viewable by the public if you do not change the site’s default privacy setting.

Keep personal information away from others by setting your security to include only friends. Verify the identity of those you correspond with.

Go through each of the privacy settings on each social media site that you frequent, and set them accordingly.

Be on the lookout for geo-tagging features and disable them. Certain sites will track your physical location via a cell phone app, providing your exact whereabouts at any given time. Posted photographs from digital cameras may have GPS coordinates embedded.

Report suspicious incidents, activity, or behavior as soon as possible.

Content

Remember that even with strictest security settings in place, certain details of your personal life, if made public, could be a security concern for you, your family, or your military unit.

Unit movements, deployments, personnel rosters, weapons information, or other command-critical information should never be posted online.

Do not share private information such as where your children go to school, home addresses, phone numbers, times and locations of events you plan to attend, or other information that allows someone to track your routines and possibly guess when and where you or your family might be.

Internet Use Safeguards (Home)

Secure your wireless network with a unique name and password.

Limit access to your wireless network so that outsiders cannot connect to it.

Ensure that antivirus, anti-spyware, and firewall software are up to date.

Do not send personal information except through encrypted links.

Avoid using public file-sharing services to transmit personal information or images.
Internet Use Safeguards (Mobile)

Assume that mobile apps and public networks are unsecure.

Consider using a virtual private network (VPN).

Change device settings to avoid automatic connection to any public network.

Do not send personal information except through encrypted links.

Cyber Attacks

Ensure that all community members understand the threat of disclosure of sensitive personal information resulting from phishing email. Advise community members on best practices for defending against this threat.

Do not click on links or open email attachments from unsolicited email.

Even when email is from a known source, consider the context of the email before responding. If necessary, verify the source of the email through an independent means.

Ensure that all sites used by the Defense Department (publicly accessible command pages, Facebook, etc.) are properly monitored and in compliance with Defense Department policy.

General Precautions (Physical and Virtual Environments)

Emphasize to community members the importance of understanding and implementing sound personal security practices to reduce their vulnerability in the surrounding community.

Limit outward signs of military affiliation (such as vehicle stickers, home decorations, using your rank in your address, or using military slang in public).

Uniformed military members present in public venues or attending publicly accessible events should exercise vigilance.

Be unpredictable with smart behavior, routines, and travel.

Be alert. Maintain good situational awareness by staying alert, knowing what to look for, and knowing what is wrong or out of place. Report all incidents of suspicious activity or behavior to appropriate authorities.
Operations Security (OPSEC)

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems
- Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Terrorists have said they are hunting people and their families at home. An Al Qaeda handbook tells its terrorists to seek out “Information about government personnel, officers, important personalities, and all matters related to those (resident, work place, times of leaving and returning, wives and children, places visited).”

Terrorist seek critical information on Army units and Army community activities to help them plan attacks. They seek to obtain the same type of information that we intend to keep from them. Examples of critical information that should NOT share on social media sites includes:

- Names and photos of yourself, your family and co-workers
- Usernames, passwords, and network details
- Job titles, location, salary, and clearances
- Physical security and logistics
- Mission capabilities and limitations
- Schedule and travel itineraries
- Social security numbers, credit cards, and banking information
- Hobbies, likes, and dislikes

---

6 AR 530-1, Operations Security
## OPSEC Do’s and Don’ts

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remember to practice computer security</td>
<td>Don’t discuss work on social media</td>
</tr>
<tr>
<td>Before posting information to a social media site consider who might have access to the data</td>
<td>Don’t use the same passwords for multiple sites</td>
</tr>
<tr>
<td>Modify personal search profile (the data about visible to others)</td>
<td>Don’t give passwords to others</td>
</tr>
<tr>
<td>Maintain reasonable suspicion about people you don’t know</td>
<td>Don’t use unsecured logon within public spaces</td>
</tr>
<tr>
<td>Verify supposed “real” friends</td>
<td>Don’t expect or depend on social media sites to offer security or protect your privacy</td>
</tr>
<tr>
<td>Watch your “friends” on social media who may post sensitive information about you or your family</td>
<td>Don’t trust Add-Ons</td>
</tr>
<tr>
<td>Be careful about accessing links and files on social media</td>
<td>Don’t be too generous with permissions</td>
</tr>
<tr>
<td>Question the utility of using social media (have you weighed the risks and benefits)</td>
<td>Don’t post information that isn’t already available to the public</td>
</tr>
</tbody>
</table>

For additional resources see the OPSEC section of the Social Media tool kit on the Antiterrorism Enterprise Portal as well as the OPSEC AKO site.⁸

Many DoD organizations have published specific procedures and policies for what can and cannot be done on computers and social networking sites. In addition, various social networking sites have published guidelines on how to protect personal information and mitigate the risks associated with social media. Unit antiterrorism officers and Army community members should know and apply these rules to help protect their units, communities, and families.
Technical Protective Measures

TECHNICAL PROTECTIVE MEASURES FOR SOCIAL NETWORKING

Use a strong password. At least 20 characters long, that is either randomly generated (like LauH6maicaza1Neez3zi) or a random string of words (like “hewn cloths titles yachts refine”). Use a unique password for each website or service you use; that way, if one account gets compromised, the rest are safe.

Use a government e-mail address. A .gov or other private-domain account will generally be more secure than a public service and will reduce the possibility of password-reset and other emails being intercepted. If you must use a public email provider, consider added precautions such as Gmail’s two-factor authentication.10

Select third-party applications with care. There are thousands of applications built by external developers that allow you to do an assortment of tasks with your account. However, you should be cautious before giving up control of your account to someone else. Revoke access for any third-party application that you don’t recognize (you can do this by visiting the Applications tab in your account settings).

Make sure your computer and operating system are up-to-date with the most recent patches, upgrades, and antivirus software and that all your computers and mobile devices are protected by secure passwords.

Change your Twitter account passwords. Never send passwords via email, even internally.

Keep your email accounts secure. Twitter, Facebook, Google+, etc., use email for password resets and official communication. Change your email passwords, and use a password different from your social media account passwords.

Review your authorized applications. Log in to Twitter or Facebook and review the applications authorized to access your accounts. If you don’t recognize any of the applications on services, contact their help center and file a security ticket.

Use extra security features. This will help keep your accounts protected. Facebook has a whole section on how to do that.

9 Excerpted from Defense Media Activity, “Guide to Keeping Your Social Media Accounts Secure,” 2015, and slightly edited
10 Google 2-Step Verification, https://www.google.com/landing/2step/
Use extra security features. This will help keep your accounts protected. Facebook has a whole section on how to do that.\textsuperscript{11}

Build a plan. Create a formal incident response plan. If your organization is a target for a phishing campaign or has been hacked, you’ll be prepared to take action and resolve the issue immediately.

Talk with your security team about ensuring that your email system is as safe as possible.

Minimize the number of people who have access to the account. Even if you use a third-party platform to avoid sharing the actual account passwords, each of these people is a possible avenue for phishing or other compromise.

Check for signs of compromise. Checking your email address and authorized apps weekly or monthly can help detect unauthorized access and address the problem before access is abused.

Change your password regularly. Changing your social media passwords quarterly or yearly can reset the clock if a password has leaked.

If you suspect a government established social media account is compromised, take the following actions:

1. Notify your chain of command immediately
2. If possible, suspend all accounts to prevent further illicit activity
3. Take the following action described below for the affected social media service

Log out of all social media sites when you are done using them!
TECHNICAL PROTECTIVE MEASURES FOR COMMON SOCIAL MEDIA APPS

Facebook

If you suspect your organization is being targeted by a phishing campaign or has been compromised by a phishing attack, it should be reported to https://www.facebook.com/hacked as well as reported through the chain of command to HQDA Public Affairs, Social Media Division. Additional help center information can be found at https://www.facebook.com/help/131719720300233/.

If you think your account was taken over by someone else, Facebook can help you secure it. The process for securing it can also help if your account or computer has been affected by a virus or malware.

For more information about staying safe on Facebook, please visit the Facebook Security Page or Help Center. Here are a few things you can do to keep your account safe:

Pick a unique, strong password. Don’t use this password for any of your other accounts and learn how to change your password. You can also use a password safe such as Lastpass, KeePass, or 1Password.

Think before you click. Never click suspicious links, even if they come from a friend or a company you know. This includes links sent on Facebook (for example, in a chat or story) or in emails. One of your friends clicking a spam link could accidentally send you or tag you in spammy posts. If you see something suspicious on Facebook, report it. You also shouldn’t download things (for example, an .exe file) if you aren’t sure what they are. Learn more about recognizing suspicious emails.

Watch out for fake pages and apps or games. Be suspicious of pages promoting offers that are too good to be true. If in doubt, check to see whether a page is verified. Also be mindful when you install new apps or games. Sometimes scammers use bad apps and games to gain access to your Facebook account.

---

12 Excerpted from Defense Media Activity, “Guide to Keeping Your Social Media Accounts Secure,” Defense Media Activity, 2015, and slightly edited
15 Facebook Help Centre, “Suspicious Email from Facebook?” http://en-gb.facebook.com/help/community/question/?id=10151675645772580
16 Facebook Help Center, “Verified Page or Profile,” https://www.facebook.com/help/196650490547892
Don't accept friend requests from people you don't know. Sometimes scammers will create fake accounts to friend people. Becoming friends with scammers allows them access to spam your Timeline, tag you in posts, and send you malicious messages. Your real friends may also end up being targeted.

Never give out your login info (such as your email address and password). Sometimes people or pages will promise you something (for example, free poker chips) if you share your login info with them. These types of deals are carried out by cybercriminals and violate the Facebook Statement of Rights and Responsibilities. If you’re ever asked to reenter your password on Facebook (if, for example, you’re making changes to your account settings) check to make sure the address of the page still has facebook.com/ in the URL (web address).

Log in at www.facebook.com. Sometimes scammers will set up a fake page to look like a Facebook login page, hoping to get you to enter your email address and password. Make sure you check the page’s URL before you enter your login info. When in doubt, you can always type facebook.com into your browser to get back to the real Facebook. Learn more about phishing.

Update your browser. The newest versions of Internet browsers have built-in security protections. For example, they might be able to warn you if you’re about to go to a suspected phishing site. Facebook supports Mozilla Firefox, Safari, Google Chrome, and Internet Explorer.

Run antivirus software. To protect yourself from viruses and malware, ensure you have a current antivirus software installation on your computer. You can learn more and download this software for free; see this Army Computer Crime Investigation Unit’s publication:

18 Facebook Help Center, “Phishing,” https://www.facebook.com/help/phishing
Configuring Facebook for a More Secure Social Networking Experience

Settings

Settings are available under the Facebook Configuration Arrow.

General Settings

Name
You can change the name of your Facebook account to just about anything; however, Facebook’s rules require that the name be your actual name. In Facebook’s own words, “We require people to provide the name they use in real life; that way you always know who you’re connecting with.” Facebook, and likely every other social networking site, does not take a serious effort to verify anyone’s identity.

The alternate name can be used for an unmarried name so friends can locate you (e.g., Susan Smith (Jones) or a nickname or diminutive of your given name). Once a name change is made, you are required to wait a period of time before another name change can be made.

1. Click Name.

2. Make changes as necessary and click Review Change.

Facebook presents a preview of how your new name change will appear on your timeline.

*This Facebook configuration guide is an addendum to CID Crime Prevention Flyer CPF-0037-14-CID361-9H

Configuring Facebook for a More Secure Social Networking Experience:
http://www.cid.army.mil/documents/CCIU/2can/CCPFFacebook.pdf
Configuring Twitter for a More Secure Social Networking Experience

Basic Notes About Twitter Configuration
Twitter is an integral thread in the fabric of the Internet. Assume that if it is posted on Twitter, it is also posted on the internet and the world will be able to see it. Therefore, do not post anything to any social media site that you do not want the world to know.

Assume that once it is posted to Twitter, and by extension the Internet, no amount of effort will eliminate it from Twitter or the Internet. The Internet does not forget. Also, there are least several sites that scrape Twitter content and keep copies of Tweets and images posted with those Tweets.

Twitter is an open platform. Participation is open to everyone with access to an Internet connection and an email address. Anyone, whether they have a Twitter account or not, can read posted Tweets unless the person posting the Tweets has configured their account to make their Tweets private.

Images on Twitter
Posting images on Twitter is generally a bad idea and should be avoided. Digital images frequently contain metadata. Although some social networking sites strip off image metadata during the upload process, Twitter does not. Image metadata can contain considerable information such as: the location where the image was captured (accurate to within a few feet), the date and time the image was captured, the make, model and serial number of the camera that captured the image, and more.

Twitter User Identities
Twitter does not vet their users. Although users are, by Twitter rules, required to use real information when they register for an account, Twitter does not verify any of that information. The extent of the verification is that someone at the email address associated with the account clicked a verification link in a received email sent by Twitter.

Later, you will see how to change settings so that you can decide who follows you. Once that setting is complete, do not accept as followers anyone you do not know or cannot verify. Social engineering is common on the Internet. Given that Twitter does not vet users, the person you think you are accepting as a follower may not be who they purport to be and could be someone trying to access personal information about you.

*This Twitter configuration guide is an addendum to CID Crime Prevention Flyer CPF-0037-14-CID361-9H
Twitter

If you suspect your organization is being targeted by a phishing campaign or has been compromised by a phishing attack, contact Twitter immediately at https://support.twitter.com/articles/185703-my-account-has-been-hacked with the word “Hacking” in the subject. Include copies of suspected phishing emails.

1. **Immediately change your Twitter password and the password** on the email associated with the account.
2. Delete any unwanted Tweets that may have been sent without your permission.
3. Go to the Applications tab of your account settings and revoke access to any apps you don’t recognize. To be absolutely sure, revoke them all and reauthorize known apps and devices by logging in from them one by one.
4. You should also check the Mobile tab of your account settings. If the phone number associated with the account is not yours, click the “Delete my phone” link at the bottom of the page.
5. Remind anyone with authorized access to your account to follow the precautions outlined on this page.
6. If you can’t access your account, file a support ticket at https://support.twitter.com/forms/hacked and email the ticket number to hacked@twitter.com.

---

18 Twitter Help Center, password reset, https://support.twitter.com/forms/hacked
Google+ and YouTube

If your Google+ and/or YouTube account has been hacked, you will need to take immediate action. Change the password for this platform immediately (through Google+).

Preventive Measures

Use added precautions such as Gmail's two-factor authentication. Any of these common actions could put you at risk of having your password stolen:

- Using the same password on more than one site
- Downloading software from the Internet
- Clicking on links in email messages

An extra layer of security. Most people have only one layer—their password—to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he’ll still need your phone or Security Key to get into your account.

Sign-in will require something you know and something you have. With 2-Step Verification, you’ll protect your account with something you know (your password) and something you have (your phone or Security Key).

Verification codes made just for you. Codes are uniquely crafted for your account when you need them. If you choose to use verification codes, they will be sent to your phone via text, voice call, or our mobile app. Each code can be used only once. See Features to learn about backup options for times when your phone is not available.

For more information, and to get access to the steps you might need to take if your account is compromised, use the Google Safety Center link.

---

Instagram

If you think your account has been hacked and you're no longer able to log in, let Instagram know.23

If your account is leaving comments or sharing things that you haven't posted, your password may be compromised.

To secure your account:

- Change your password or send yourself a password reset email24
- Revoke access25 to any suspicious third-party apps

Note: Never grant third-party access to a website or apps that aren't following Instagram's Community Guidelines26 or Terms of Use27 (including websites selling or promising free followers or likes), as it's likely an attempt to use your account in an inappropriate way.

---

25 Instagram Help Center, “How Do I Stop Sharing My Instagram Posts to Another Social Network?” https://help.instagram.com/536741816349927?sr=1&query=revoke%20access&sid=OnazdIk3z9jVHpWr
Flickr

Flickr is a photo- and video-sharing community run by Yahoo. Millions of members from all over the world are uploading photos and video that they have created, each sharing their unique view of the world.

When using Flickr you can post, sort, and share photos and videos you have created with friends, family, and folks from around the globe.

**How to customize your privacy controls:** Flickr empowers the community to control access to content by providing multiple options for adjusting privacy settings on photos, your Flickr profile, and even on commenting and contact preferences. To review these settings, visit your Flickr account page. Some important sections:

**Profile settings.** You can control your profile privacy settings to dictate who is able to see different parts of your profile.

**Change a password.** For a Yahoo account, you can change your password, or request a new password, at https://edit.yahoo.com/forgotroot/.

**Commenting controls.** You control who can comment on your public photos and videos. By default, anyone is able to comment on your photos. You can change this in the privacy setting for comments. If someone posts a comment you don’t like, you can just delete it.

**Post with care:** The Flickr community is ever growing. As you upload content, be sure to know which privacy settings you have selected and how visible the content will be to the general public. You can also choose to opt out of your content being searchable on third-party sites.

**Block unwanted individuals:** Sometimes we just don’t want to interact with someone. If you block a community member, that person can no longer interact with you or your photos. There are three ways to block a person:

1. Click the “Block [membername]” link on the Person menu.
2. Click the “Block this person?” link on the person’s profile page.
3. Delete a comment on one of your photos. (You’ll see the option to block the person, too.)
4. To see the people you’ve blocked, click the link at the bottom of your contact list.

**SafeSearch:** You can control what kind of content shows up on your Flickr searches. By default, SafeSearch is enabled on your account, which leaves restricted and

---

28 Flickr sign-in, https://www.flickr.com/
moderate content out of the results. When you are signed in, this feature can help ensure that your audience is not exposed to “adult content.”

**Report abuse:** The Flickr staff works with the community to ensure an enjoyable experience for all. If you see something you feel violates the Terms of Service or the Community Guidelines, report it by doing the following:

*Flagging a Photo*

1. Go to the photo’s page.
2. At the bottom-right corner of the page, click Flag This Photo.
3. Check the “I don’t think this photo is flagged at the appropriate level” checkbox.
4. Click Submit.

The Flickr staff will review the photo in question.

If you come across content that you think might be illegal or prohibited, use the **Report Abuse system**[^1] instead.

**Reporting Abuse**

1. At the bottom of any Flickr page, under “Community,” click Report abuse.[^2]
2. Select the issue from the pull-down menu.

LinkedIn Help Center: https://help.linkedin.com/app/home

LinkedIn

See the Army Computer Crime Investigation Unit’s publication “Configuring LinkedIn for a More Secure Professional Networking Experience”: http://www.cid.army.mil/documents/CCIU/2can/CCPFLinkedIn.pdf
Additional Resources

Below is a list of the resources to assist antiterrorism officers, family readiness groups, and Army community members from the risks associated with the use of social media.

Also, add the below resources:

**Defense Media Activity, Guide to Keeping Your Social Media Accounts Secure, 2015:**

**Army One Source Website (see Family Programs and Services, go to, iWATCH Army – “See Something Say Something” section):**

**Antiterrorism Enterprise Portal:** On Internet Explorer, select the Defense Department email certificate in order to gain access.

**U.S. Army Criminal Investigation Command's Computer Crime Investigation Unit:** Additional social networking safety tips and resources can be found in the Cyber Crime Prevention Flyer “Social Networking Safety Tips” at

**Antiterrorism Level 1 Training:**

**Army Operations Security Facebook page:**

**Army Operations Security Support Element web page:**

**Army Operations Security Support Element Family Readiness web page:**
iSALUTE: Suspicious activity can be reported to U.S. Army Counterintelligence through iSALUTE or by calling **1-800-CALL-SPY (1-800-225-5779)**. ISALUTE can be accessed at [https://www.inscom.army.mil/isalute](https://www.inscom.army.mil/isalute)

Additional information on technical and behavioral best practices that can be implemented to mitigate risks of using social networking sites can be found at the following websites:

Social Media Education & Training:

FBI Internet Social Networking Risks:

On Guard Online:
[www.OnGuardOnline.gov](http://www.OnGuardOnline.gov)

U.S. Computer Emergency Readiness Team (CERT):
[www.us-cert.gov](http://www.us-cert.gov)

Internet Crime Complain Center (IC3):
[www.ic3.gov](http://www.ic3.gov)

---

33 FBI Counterintelligence, “Internet Social Networking Risks,”
Smart Cards

Social media Smart Cards assist users of social media with proper configuration of account privacy and security settings. These cards are available on the Antiterrorism Enterprise Portal and Army One Source website (see additional resources section for websites).

Facebook

Twitter