

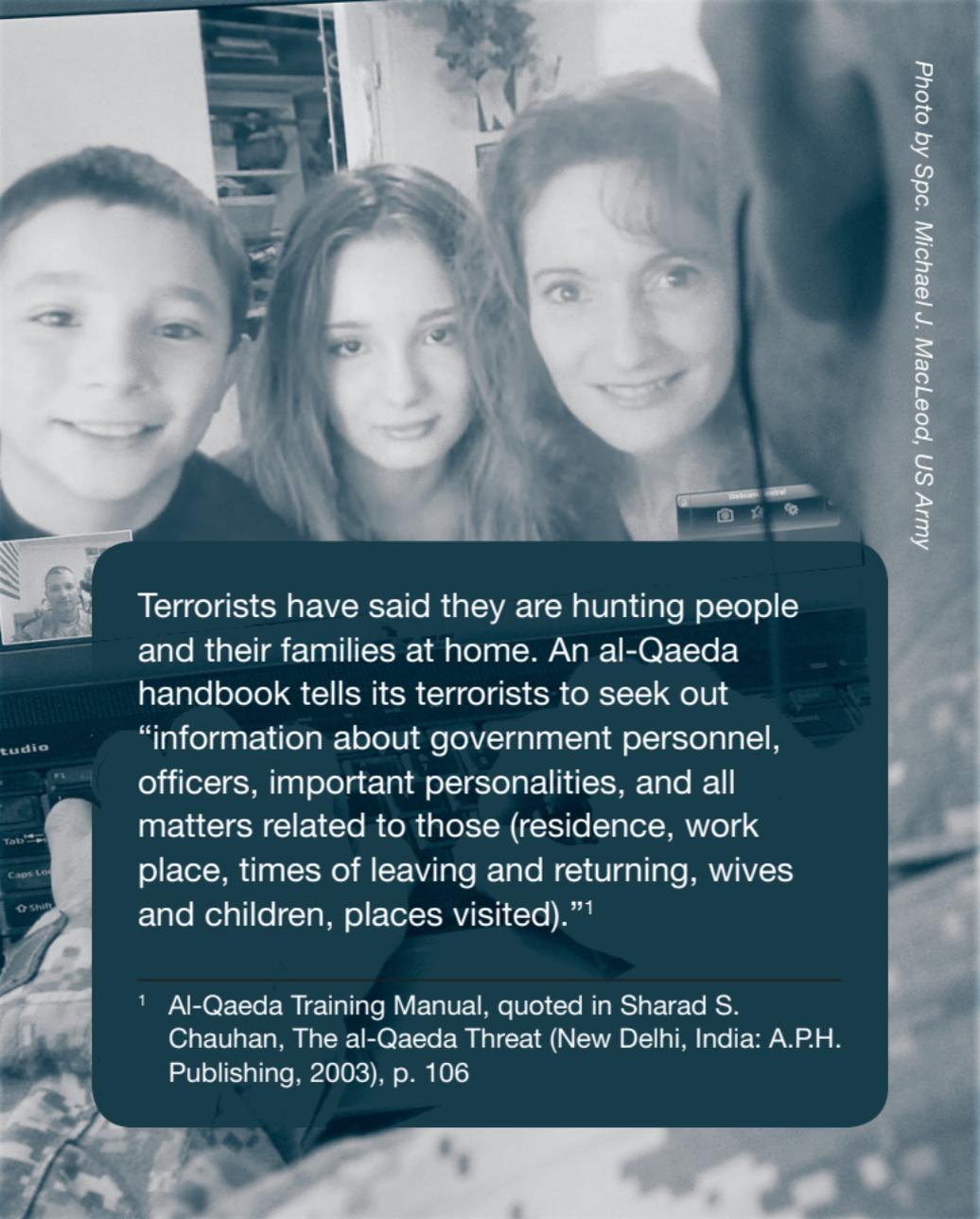


ANTITERRORISM AWARENESS
FOR SOCIAL NETWORKING

AUGUST 2015



U.S. ARMY



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 (residence, work place, times of leaving and returning, wives and children, places visited).”¹

¹ Al-Qaeda Training Manual, quoted in Sharad S. Chauhan, *The al-Qaeda Threat* (New Delhi, India: A.P.H. Publishing, 2003), p. 106

PURPOSE

This pocket guide provides precautionary and protective measures designed to mitigate the risk of using social networking sites.

BACKGROUND

In light of the threats on social media against Soldiers and their families by terrorist organizations such as the Islamic State of Iraq and the Levant (ISIL, also called ISIS), the Department of the Army has published social media messages and precautions. This pocket guide provides precautions and recommended practices to help protect our Soldiers and families.

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.”²

² National Security Agency, Systems and Network Analysis Center, Information Assurance Directorate, “Social Networking Sites,” <https://www.nsa.gov/ia/files/factsheets/I73-021R-2009.pdf>

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.”³ In fact, social networking sites can present an operations security risk to military units and a direct risk to the individual.

³ National Security Agency, “Social Networking Sites”

GENERAL PRECAUTIONS

- Use strong, unique passwords. Consider using passphrases for an additional level of security.
- Change your password regularly.
- Use a government e-mail address whenever possible.
- Make sure your computer and operating system are up-to-date.
- Keep your email accounts secure.
- Review your authorized applications.
- Use extra security features.
- Minimize the number of people who have access to the account.
- Check for signs of compromise.
- 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.
- 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.

- 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.

Login

Password



HOME INTERNET USE SAFEGUARDS

- Keep your antivirus software current.
- 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.



Not just the First Responders...
First Preventers Protecting Across the
Spectrum of Military Operations.



**SOCIAL MEDIA FOR
ANTITERRORISM AWARENESS
AND COMMUNITY OUTREACH**

MOBILE INTERNET USE SAFEGUARDS

- 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.



OPERATIONS SECURITY (OPSEC)

Terrorists seek 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 information that you should NOT share on social media sites:

- 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

SOCIAL MEDIA OPERATIONS SECURITY DO'S AND DON'TS

Do's	Don'ts
Practice computer security	Don't discuss work
Before posting information to a social media site consider who might have access to the data	Don't use the same passwords for multiple sites
Modify your personal search profile (the data about you that is visible to others)	Don't give passwords to others
Maintain reasonable suspicion about people you don't know	Don't use unsecured logon within public spaces

Do's	Don'ts
Verify supposed "real" friends	Don't expect or depend on social media sites to offer security or protect your privacy
Watch your "friends" on social media who may post sensitive information about you or your family	Don't trust add-ons
Be careful about accessing links and files on social media	Don't be too generous with permissions
Question the utility of using social media (have you weighed the risks and benefits?)	Don't post information that isn't already available to the public

TECHNICAL TIPS ABOUT PRIVACY SETTINGS

- 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.
- Remember that even with the 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.

RESOURCES

- **Antiterrorism Enterprise Portal:** On Internet Explorer, select the Defense Department email certificate in order to gain access.
<https://army.deps.mil/army/sites/PMG/OPMG/OPS/antiterror/ATEP/default.aspx>
- **Army OneSource Website** (see Family Programs and Services, “Go To,” iWATCH Army—“See Something Say Something”): <http://www.myarmyonesource.com/default.aspx>
- **U.S. Army Criminal Investigation Command, Social Network Safety, How to Protect Your Identity Online:** <http://www.cid.army.mil/documents/Lookout/Social%20Network%20Safety.pdf>
- **Army Operations Security Facebook page:** <https://www.facebook.com/pages/Army-Operations-Security-OPSEC/163005357133404?ref=hl>

- **Army Operations Security Support Element web page:** <https://www.us.army.mil/suite/page/589183>
- **Army Operations Security Support Element Family Readiness web page:** <https://www.us.army.mil/suite/page/594109>



**ARMY
STRONG®**



Always Ready, Always Alert
Because someone is depending on you

