

**SOMEONE**

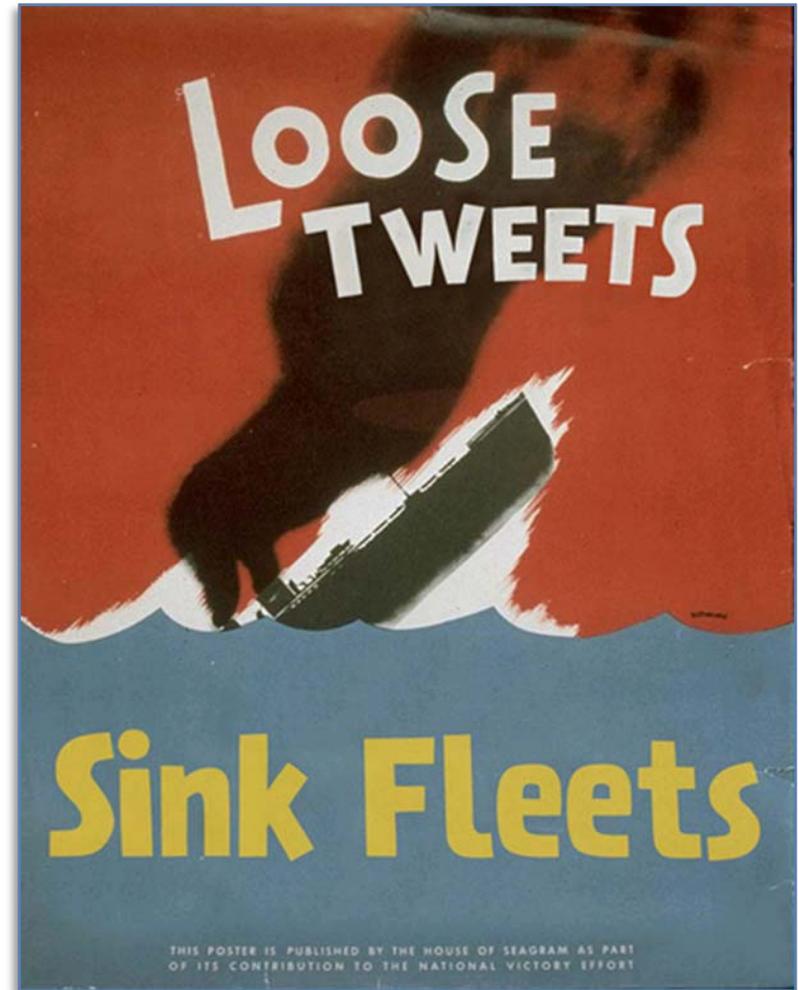
**SOCIAL MEDIA SNAPSHOT**

OPERATIONS SECURITY  
(OPSEC)

**TWEETED!**

# WE ALL KNOW THAT “LOOSE LIPS SINK SHIPS” AND ...

Social media amplifies OPSEC risks because it enables **greater volume** and **increased speed** of information shared publically.



# The threat is real.

The Scoop Deck blog shed light on a Dec. 2009 Al-Qaeda call for their members to monitor what we say about ourselves, our units and our families online in order to gather intelligence.

“Information on every U.S. Naval unit should be quietly gathered... their ranks, what state they are from, their family situation, and where their family members live...  
...search for the easiest ways of striking these ships.... Do not underestimate the importance of any piece of information, as simple as it may seem....”

NavyTimes  
**SCOOP DECK**

The terror threat at sea  
DECEMBER 11, 2009 | BLOGS SHEDDING OPERATIONS BACK THE HIDEOUT BAY | PHOTO BY CHALMERS



A boarding team from the destroyer Leahon approached a suspicious small boat in the Red Sea in July. Internet chatter about at-sea terror threats has increased this week. Many...  
...sudden, there is lots of discussion online about terrorist threats to U.S. warships in the Middle East. Defense has [struggled](#) [last](#) [week](#) [today](#) about a new warning for ships, including this money quote: "We assess a direct, grave threat, to al Qaeda, against U.S. Navy warships and U.S.-flagged vessels. Moreover, if U.S.-flagged merchantmen are still steaming area here in the U.S. 5th Fleet area of responsibility without armed security, they do so now at a considerable elevated risk."

There's more: Richard Washel, a spokesman for the Middle East Media Research Institute, tells Scoop Deck that a post on a jihadist web site Wednesday called for people to "gather intelligence" about the U.S. and international warships that patrol the Gulf of Aden, the Arabian Sea and the Persian Gulf. Here's the whole post, provided by Washel:

**WHAT THEY WANTED:** The call wasn't just about unit missions, location, troop manning, weapons, movement and route. They asked for members' names, ranks, home state, family situation and family names.

Managers of official social media presences have an added responsibility to:

- Identify information that may compromise OPSEC (*and remove it*)
- Inform Sailors, family members and fans/community members of OPSEC best practices

**So what things should you look for?**

# 1. Sailors or family members sharing too much information



Looking for some assistance. Currently in Afghanistan, oldest boy is in the boy scouts and he is working on his "Signaling" merit badge. Was wondering if there are any "Signalpersons" in the Illinios area, about 90 miles south of Chicago. Thank you for any help.

## ***DANGEROUS:***

- My Sailor is in XYZ unit at ABC camp in ABC city in Iraq.
- My daughter is aboard the XYZ ship heading to ABC city/country in X days.
- My family is back in Union, KS.

## ***SAFER:***

- My Sailor is deployed in Iraq.
- My son is aboard the Stennis.
- He is coming back sometime in May.
- I'm from the Midwest.

**BEST PRACTICE:** Protect your yourself and your family. Avoid providing details about yourself, especially related to a current deployment. Avoid providing details about your family.

## 2. Posts about scheduled movements and current or future locations of ships or units



The screenshot shows a social media post and a reply. The main post features a profile picture of a globe and the text: "The U.S.S. Tortuga departs from Okinawa tomorrow! Wishing them safety!!" with interaction options "3 hours ago · Comment · Like · Report". A reply from a user with a profile picture of a group of people says: "Loose lips -- sink ships! May not want to post anything about ships movement, I am sure that people that mean to do the US Military harm are monitoring these websites." with interaction options "3 hours ago · Delete · Report".

### ***DANGEROUS:***

- My daughter is aboard the XYZ ship heading to ABC city/country in X days.
- She will be back on X date from XXX city.

### ***SAFER:***

- My son is aboard the Stennis.
- He is coming back sometime in May.

**BEST PRACTICE:** To be safer, talk about events that have happened not that will happen, unless that information has been released to the media. Otherwise, don't provide specific details ship movements.

# 3. Detailed personal information

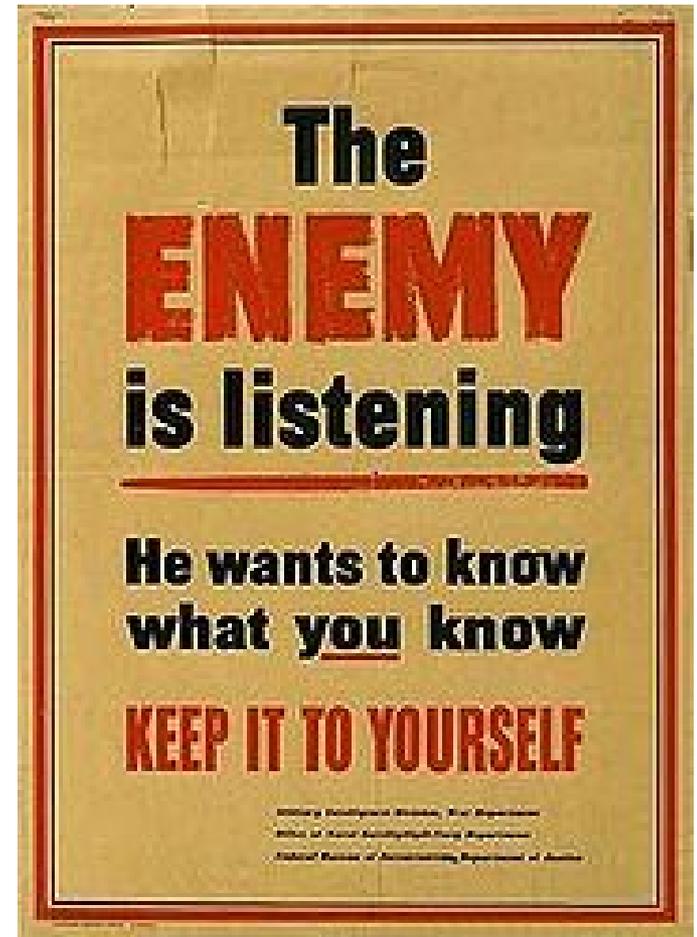
The image shows a screenshot of a Facebook profile page. The profile picture is a person in a military uniform, with a white box redacting their name. The page includes a search bar, a navigation bar with 'Wall' and 'Info' tabs, and a privacy notice. The 'Basic Information' section shows 'Sex: Male'. The 'Education and Work' section is circled in red and lists: 'College: '95 nuclear engineering', 'High Schools: High School '88', 'High School '88', 'Employer: United States Navy', 'Position: Information Warfare', 'Employer: Defense Intelligence Agency', and 'Position: Watch Officer'. The 'Pages' section shows 'Paris Hilton'.

**BEST PRACTICE:** Share information about yourself smartly and be careful what you disclose about your family and occupation. Use privacy settings to protect your personal info.

# Sailors and their families should also be particularly careful not to share:

- Spouse's deployment status
- Home address
- Telephone numbers
- Location information
- Schedules

*Your close friends and family members have this information, so there is no need to post online.*



## Other information that should not be shared:

- Descriptions of overseas bases
- Unit morale
- Future operations or plans
- Results of operations
- Discussions of areas frequented by service members overseas (even off-duty hangouts)
- Daily military activities and operations
- Technical information
- Details of weapons systems
- Equipment status

# Well, gosh, what's ok to share?

- Pride and support for service, units, specialties, and service member
- Generalizations about service or duty
- Port call information after it has been released to media
- General status of the location of a ship at sea (“operating off the Coast of San Diego” as opposed to “45 nm north of San Diego”)
- FPO addresses for units
- Any other information already in the public domain

# What should you do if you identify information online that risks Operations Security?

- Record and archive the information and remove it if possible.
- Notify your command of any potential OPSEC violation.
- Inform the individual of the OPSEC violation. Use this as a teachable moment and provide him/her with OPSEC best practices and resources so they don't repeat this mistake.
- Educate your community/fan base of what OPSEC is, why it's important, and what they can do about it if they think they know of a violation.

**YOUR DUTY:** As managers of official social media presences that connect our stakeholders with our commands, it is your responsibility to monitor for OPSEC issues and continue to educate audiences about OPSEC.



# Naval Operations Security Support Team provides educational materials you can share with your command and family members

facebook



Search



Videos Posted by Naval Operations Security (OPSEC)

[Previous](#) | [Last](#)



**Apr 26, 2010 10:24am**

by Naval Operations Security (OPSEC)  
(videos)

**1:00**

Share

[View in High Quality](#)

[Report Video](#)

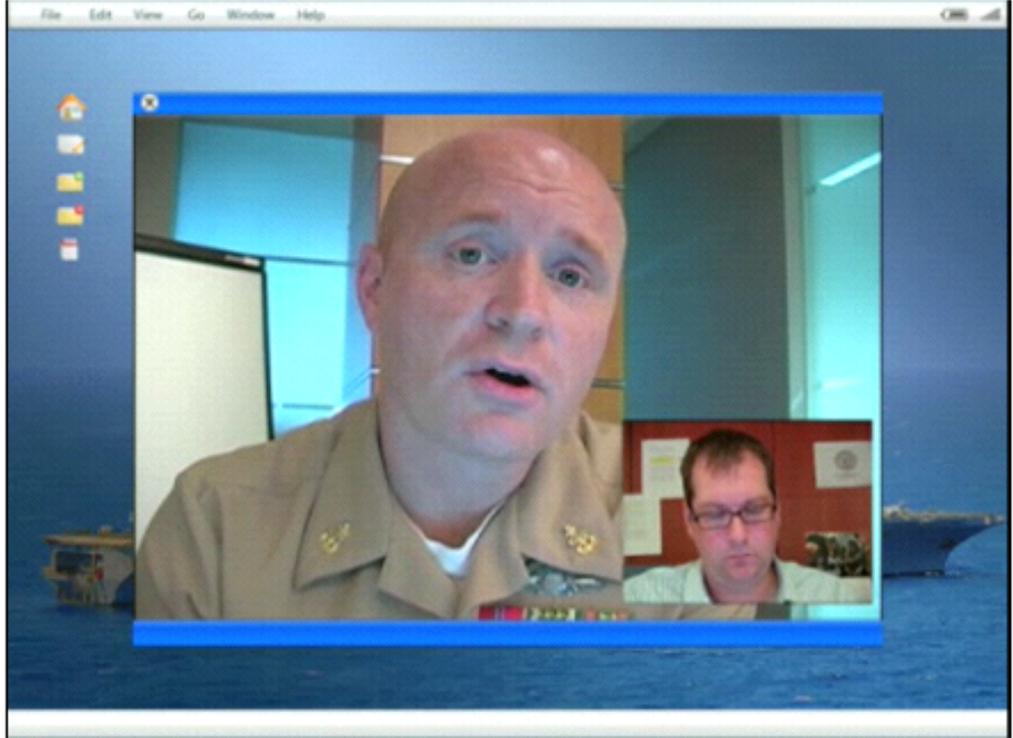
<http://www.facebook.com/NavalOPSEC>

# NavyForMoms also has informative OPSEC resources for families

OPSEC tips from Senior Chief Tom Jones, Navy Recruiting Command:

- **Use different screen names** if you have profiles on different social networking sites
- **Do not add names or locations** to photos posted online
- **Be careful of what images are in the background** of photos posted so not to post images with Navy equipment or landmarks that could identify your location

<http://navyformoms.ning.com/video/opsec-internet-safety>



The screenshot shows a video player interface. At the top left is the "NAVY For Moms" logo. To its right is the video title "OPSEC & Internet Safety" and the text "Added by [Navy for Moms Admins](#) on August 27, 2009 at 11:01 am". Below the title is a "View Videos" link with a play button icon. The video player itself shows a man in a tan Navy uniform speaking. In the background of the video, another man with glasses is visible at a desk. The video player has a standard menu bar with "File", "Edit", "View", "Go", "Window", and "Help".

# Additional OPSEC Resources

- U.S. Strategic Command (STRATCOM) -- [Social Networking OPSEC Training](#)
- Navy Information Operations Command (NIOC) Norfolk -- [Social Networking OPSEC Brief](#)
- [MCPON to Sailors: Be Smart about Online Threats](#)
- [The Basics: Protecting Personal and DoD Information](#)
- [Navy Information Operations Command](#) website
- CHINFO [Social Media Resources Page](#)
- [Naval OPSEC Support team on Facebook](#)
- [Navy for Moms OPSEC video](#)