References

- DTM 2009-026 Responsible & Effective use of Internet-based Capabilities
- SECNAVINST 5720.47B DON WWW Web Policy
- DON CIO_CHINFO Joint Memo 10_Oct 07_DOC Web Presence Policy
- NTTP 3-54 M Operations Security
- DOD Directive 5205.2 OPSEC Program
- OPNAVINST 3432.1 Operations Security
- DON Navy Public Affairs Policy & Regulations SECNAV 5720.44B
- DON Policy for Content of Publicly Accessible World Wide Web Sites SECNAV 5720.47B
- COMNAVREGMIDLANTINST 5720.1 Web 2.0 Technologies
- ALNAV 056-10 IbC- Official Internet Posts
- ALNAV 057-10 IbC- Unofficial Internet Posts
OPSEC is a process that identifies critical information, outlines potential threats and risks and develops counter measures to safeguard critical information.
Critical Information

- Information we must protect to ensure success.
- Information the adversary needs to prevent our success.

- Names and photos of you, your family and co-workers
- Usernames, passwords, network details
- Job title, location, salary, clearances
- Physical security and logistics
- Position, mission capabilities and limitations
- Operations & missions
- Schedules and travel itineraries
- Social security number, credit cards, banking information
- Hobbies, likes, dislikes, etc.
Data Aggregation

- Information collection from multiple sources
- Al Qaeda handbook: open and legal public sources accounts for 80% of all information collected
- Legal and illegal collection methods
Methods used to obtain Critical Information:

- Unprotected communications
- Sharing too much with strangers
- HUMINT Observations
- Technology
- Trash
- Media
- Email
- Web pages
- Social Networking Sites

Illegal methods are OK with adversaries!!!
Social Networking

Social Networking Sites (SNS) allow people to network, interact and collaborate to share information, data and ideas without geographic boundaries.
Revised Statement of Rights & Responsibilities

- “You own all of the content & information you post.”
- “You specifically give us the following permission, subject to your privacy and application settings, to use any content that you post on or in connection with Facebook.”
  - Non-exclusive
  - Transferable
  - Sub-licensable
  - Royalty-free
  - Worldwide license
- “We may collect information about you from other users.”
- “Sometimes we share aggregated information with third parties.”

Consent to Collection and Processing in the United States. By using Facebook, you consent to having your personal data transferred to and processed in the United States.
Why use a SNS?

Personally
- Entertaining
- Maintain Relationships
- Network
- Centralized information

Professionally
- Marketing/recruiting
- Public Relations
- Connect with customers
- Solicit ideas and feedback
The Danger

Bad guys use it, too:

- Stalkers
- Thieves
- Terrorist
- Hackers
- Phishers/Scammers
- Enemy organizations
- Pedophiles
- And the list goes on…
The Danger

Al-Qaeda communiqué December 2009:

“The affair with the U.S. Navy began several years ago, when the lions of Al-Qaeda struck the destroyer U.S.S. Cole, in Yemen; now, with Allah’s help, all the American vessels in the seas and oceans, including aircraft carriers, submarines, and all naval military equipment deployed here and there that is within range of Al-Qaeda’s fire, will be destroyed…

“To this end, information on every U.S. naval unit – and only U.S. units!! – should be quietly gathered [as follows: the vessel’s] name, the missions it is assigned; its current location, including notation of the spot in accordance with international maritime standards; the advantages of this naval unit; the number of U.S. troops on board, including if possible their ranks, and what state they are from, their family situation, and where their family members live; what kind of weapons they carry; the [vessel’s] destination…; which naval units are closest to Islamic countries; which naval units are close to Western countries in general, searching all naval websites in order to gather as much information as possible, and translating it into Arabic; 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…..
The following is a security awareness statement signed by the Chief of Security, Pentagon Chief Information Officer, OSD Network Directorate:

Question 14 of the National Agency Questionnaire (SF-86) asks for names of your relatives and associates. The term associate is defined as any foreign national that you or your spouse are bound by affection, obligation, or close and continuing contact.
DO’S & DON’TS of SOCIAL NETWORKING
“Do’s”

Do: Remember Computer Security
Do not be an easy target for computer crimes

• Hacking
• Theft
• Planted code
• Antivirus software
• Firewalls
• Strong Passwords
• Permission Settings
“Do’s”

Do: Verify All Friend Requests
Social engineering and “conning” starts with a friend request

Adversaries can get the data from:
• Free people search engines
• Other SNS’s
• Your posts/profile
• Your friends posts/profile

Verify Requests Before Approving!
“Do’s”

Do: Utilize All Available Privacy Settings

Customize available settings to be as secure as possible

• “Everyone” may be accessed by anyone with access to the internet

• How many security settings are available on Facebook?
  Over 120
“Do’s”

Do: Watch Your Friends Settings

Sure your profile is secure, but what about your 115 friends profile settings?
Do: Closely Monitor Your Children’s Use of the Internet

- Cyber-bulling
- Kidnapping
- “Sexting”
- Stalking
- Pedophiles
  - 500,000+ registered sex offenders in the USA
  - 95,000 registered sex offenders profiles on Myspace
“Do’s”

Do: Verify Links & Files Before Executing

Would you follow a link in e-mail? Would you download and run an attachment? Then why do you do these things on SNS’s?

- Phishing scams
- Malicious coding
- Viruses
- Scareware

Verify before executing!
“Do’s”

Do: Blog with Caution

- Avoid details, don’t get personal
- Who is reading your blog?
- Lessons learned 101 for the adversary
“Do’s”

Do: Understand the Risks Associated with Geotagging

- Location/GPS data attached to photos
- Feature in Smartphones and digital cameras
  - Lat/Long
  - Device details
- “Check-in” feature
  - Facebook Places
  - Google Latitude
  - Foursquare
  - Gowalla
“Do’s”

Do: Be an Informed User of a SNS

• How much personal information do you broadcast?
• Are you very careful about what details you post?
• Do you understand data aggregation issues?
• Are you willing to find and learn all the security settings and keep up with them as they change?

Are you willing to accept the risk?
“Do’s”

Do: Have a Contingency Plan

- KIA, MIA, POW
- What details will the adversary have to use against you?
- What information will the media have access to?
- Power of Attorney
- Memorial pages
“Do’s”

Do: Assume the Internet is FOREVER

• There is no true delete on the internet
• WWW means World Wide Web
• Every Picture
• Every Post
• Every Detail
“Do’s”

Do: Understand Official DON Guidance That Governs Military Personnel Use of SNS’s

- DON ALNAV 056/10 Official Internet Posts
  - Social media posts in an official capacity
- DON ALNAV 057/10 Unofficial Internet Posts
  - Any content posted about the DON by DON personnel in an unofficial & personal capacity
  - DON personnel are responsible for all DON-related content they publish on the internet
“Don’ts”

Don’t: Use the Same Passwords

- Hackers count on users using the same passwords for multiple accounts
- Password1 is not a strong password
“Don’ts”

Don’t: Depend on SNS’s Security Settings

But it’s set to private … right?

- Hackers
- Incorrect or incomplete settings
- Sale of data
- Upgrades/site changes
- “Risks inherent in sharing information”
- “USE AT YOUR OWN RISK. We do not guarantee that only authorized persons will view your information.”

UNCLASSIFIED
“Don’ts”

Don’t: Trust Add-On’s or Applications

• Plugins, Games, Applications
  – Third Party Software
  – Applications designed to collect data
  – Malicious code
  – Separate terms of use & privacy
  • “We are not responsible for third party circumvention of any privacy settings or security measures.”
“Don’ts”

Don’t: Grant the Same Access to Everyone

- Don’t treat all Friends equally
- Control & customize individual access
- Do create groups
  - Poker club
  - Family
- Set permissions for everything:
  - Your status
  - Photos
  - Postings
“Don’ts”

Don’t: Discuss Details

• Never post anything you would not tell directly to the enemy
• Never post private or personal information—no matter how secure you think your settings are
• Assume the information you share will be made public

Details make you vulnerable
Questions?

Please contact the NOST for assistance or any of the following:

- Computer-based training
- FRG/Ombudsman support
- OPSEC & other tailored briefs
- Videos, posters, brochures & fliers
- OPSEC Reminder Cards
- Two-day Navy OPSEC Officer course
- General OPSEC support
- Other Resources

Countries don’t have friends...

They have interests. Which country is interested in what you do?

Naval OPSEC Support Team
opsec@navy.mil
757-417-7100
www.facebook.com/NavalOPSEC
www.twitter.com/NavalOPSEC
www.slideshare.net/NavalOPSEC

UNCLASSIFIED