

What is Operations Security (OPSEC) and why should I care?

OPSEC for Travelers

By OPSEC Coordinator

NAWSCL OPSEC Office 760.939.5025

Many people believe that if information is not classified, it is okay to share. However, this is not at all accurate. Let's look at an example involving unclassified information. Would you post your full name, birth date, and social security number on a bulletin board or website? Would you tape the code to your home's alarm system to the front door? Of course not! If any of the information classified? No, but you understand the harm that could come from sharing that information with strangers, so you keep it secure. Whether you have realized it or not, you have been practicing OPSEC!

OPSEC is not just about work

OPSEC focuses on identifying and safeguarding exactly this type of sensitive or critical information, whether it's about you, your family, your overall mission, or your day-to-day operations. We all have

Continued on page 2

INSIDE THIS ISSUE

- 1 What is Operations Security? Continues on Pg 2
- 1 Cyber Security Awareness Continues on Pg 3
- 4 Questions & Answers



Cyber Security Awareness

What to Post on the Social Media

By IAM

NAWSCL IAM Office 760.939.1233

The policies and guidelines on what information is appropriate to share on social media are different for the Department of Defense pages and your personal pages.

Are you guilty of putting out too much information?

Mixing personal life with professional profile is never a good idea because when you do, you put yourself in a bind with trust issues. Over-sharing department activities may be a violation of the non disclosure agreement between you and the department.



Engaging in social networking rage, avoid cruel or hurtful posts, reflects your professionalism and your department. What you do outside of work also reflects your highest ranking official.

Posting classified or sensitive information, your security clearance level, personal views listed as those of your department or your personally identifiable information (PII) on the social media is asking for trouble. Not only are you endangering yourself but others.

Believing to have the most connections wins is a false sense of cyber popularity.

Password laziness is a good way to get your profile hacked into. Use strong passwords for your protection and your department's security realm.

access to this type of information. Whether we realize it or not, every day there are adversaries trying to gain this information. Their analysts are piecing together small bits of data to determine the big picture related to our missions. OPSEC ease a proven, analytic process we can use every day to make sure this does not happen. Your understanding and use of sound OPSEC practices may just save lives.... including your own!

The Five Steps of OPSEC Process

These steps will help you better protect yourself, your family and your mission. They are:

1. Determining what your critical information really is so that you're protecting the right information;
2. Determining who our adversaries are - those individuals, groups, or countries who pose a real threat to us;
3. Identifying our vulnerabilities - weaknesses that adversaries will try to take advantage to learn our information;
4. Assessing ourselves to determine what level of risk we are actually facing; and finally,
5. Implementing countermeasures, or figuring out what to do to lower the risk.

OPSEC applies to everyone

Remember OPSEC applies to everybody. Whatever your job, wherever you travel, you know sensitive information that the "bad guys" would like to have. Our collective job is to figure out what that information is and then protect it from those who want to do us harm.

Putting it All Together

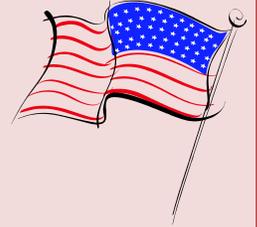
OPSEC is not just an add-on to security programs. It is about making sure that you and your mission are secure 24 hours a day, seven days a week. As government employees, it is rare to receive information designed to help you keep yourself and your family safe at home, but as OPSEC professionals we recognize that a vulnerable family makes a vulnerable employee, which leads to a vulnerable mission. This is not something that can be done for you, however all we can do is give you the tools and help you help yourself.

It is vital that you recognize that every person involved in your mission, including family members must be

vigilant. Careless action by any one person can endanger your team or family. You do not need to become paranoid, just be aware of the threats and do your part to counter them. We must all work together in order to succeed.

Basic Critical Information for Travel

- Travel arrangements;
- personal data;
- copies of orders, if issued;
- specific travel location;
- General mission information;
- names or photos of fellow travelers/unit members;
- medical information; and,
- Financial arrangements.



Simple Countermeasures for Travel

- Do not discuss travel plans outside the immediate family.
- Do not post travel plans on social networking sites.
- Be circumspect when communicating with family while you travel. Save the detailed stories and pictures for when you get home.
- Clean out your wallet and suitcase before you travel.
- Use a cross cut shredder to dispose of unneeded travel documents (spare copies).
- Educate yourself! Be aware of the threats and vulnerabilities off your travel location.
- As much as possible, keep two standard routine prior to travel. Do not advertise that you will be away!

Remember it is all about safeguarding the information. Protect yourself, your family, your missions, and your information.

If you still ask, what information? It is said that the less you know, the less is revealed. ❖

Did you know?

A US government official on sensitive travel to Iraq created a security risk for himself and others by tweeting© his location and activities every few hours.

A family on vacation kept friends up to date via online profiles; their home was burglarized while they were away.

Over 90,000 registered sex offenders were removed from one popular social networking site (SNS), and those were the ones who used their real names.

New computer of viruses and Trojans that successfully target information on SNSs are on the rise.

Several kidnapping, rape and murder cases were linked to SNSs where the victims first connected with their attackers.

Some foreign investors, including government and commercial entities known to be involved with organized criminal activity, own large stakes in certain SNSs.

Information in SNS profiles has led to people losing job offers, getting fired, and even being arrested.

SNSs have become a haven for identity thieves and con artists trying to use your information against you.

According to the Al Qaeda Handbook, terrorists search for data about "government personnel, officers, important personalities, and all matters related to them (residents, workplace, times of leaving and returning, and children, places visited."

Trigger finger, clicking on anything and everything, can be risky. Public social networking sites generally do not have secure login available (HTTPS with the lock icon).



What You Don't Know **Can Hurt You!**



Remember, **Ignorance** is Never an **Excuse!**

Social networking site (SNSs), like Facebook© and Twitter© are great ways to connect with people, share information, and market products and services.

However, these sites can also provide adversaries, such as criminals, spies, and terrorists with the critical information they need to disrupt your mission and harm you, your coworkers, or even your family members.

The more information adversaries can obtain, the more opportunities they have to cause damage at your expense.



**BE PART OF THE SOLUTION,
NOT THE PROBLEM!**



SECURITY BREAK

The words "Objects in the mirror are closer than they appear" is required by Congress to be on all convex side-view mirrors on American cars; but the use of SF 702 (Security Container Check Sheet) to record the opening and closing actions on a security container is required by

- Congress
- Department of Commerce
- Department of State
- Department of Defense.

d. Department of Defense



**Don't let carelessness
blow your career, protect
our nations secrets**

Be Safe Be Smart Online and Offline

Protecting your Critical Information

Your critical information is any information that you or your supervisor considers sensitive. Here are some examples:

- Names and photos of you, your family and co-workers;
- Job title, locations, salary, grade, clearance status;
- Work or personal addresses and phone numbers;
- Usernames, passwords, computer and networking information;
- Operational, security, and logistical data;
- Mission capabilities or limitations;
- Schedules and travel itineraries;
- Interests, hobbies, likes, and dislikes; and,
- Social security numbers, credit card, and banking info. ■

Do not post critical information: if you do not want it public, do not post it. Search engines and functions make it easy for adversaries to find what they are interested in. Once information is on the Internet, it is there forever.

QUESTIONS AND ANSWERS

Q: Who might the adversary be?

A: The adversary could be the drug dealers, the media (newspaper, radio), the Public Relations office, the official who provided the data to the PR, foreign entities, your enemy, uncleared personnel, criminals, etc. The list goes on.

Q: Why do I need a sponsor to get my security badge or get it renewed?

A: Many DON policies have been updated due to the continuous need to protect DON assets and to ensure you are given the proper authorization for certain areas.

Q: What I put on my Facebook pages is my business, so why should I take my photos down especially the one where I'm posing with an assault rifle? I want everyone to know I'm showing off my best toy.

A: It is okay to pose however you wish to pose but while you are employed by the DON/DOD, you will follow the personal conduct standards outside of work as well. Posing with an assault rifle and giving "signs" indicate reliability, judgment,



NETWORK SECURITY
Do your part by taking
cautionary steps while
utilizing the internet.

and trust issues. Not only is your job on the line, but your security clearance eligibility too. And worse, you are attracting possible criminals. Someone with a "toy" like that is asking for trouble; think of the safety of your family, your home, your work, yourself.

Q: Why can't I post "critical" information when it is already on the internet?

A: Because the "critical" information already on the internet most likely went through a security review before it was put on the internet. Remember you, as a DON/DOD employee, signed a non disclosure agreement and all information are property of the U.S. government. The critical information revealed could be used against you. Protect all critical information.



MALICIOUS

COMPUTER CODE 101



WORM: An independent program. Reproduces by copying itself from one computer to another, usually over networks. Harnesses resources, shuts down networks.



VIRUS: Code fragment that copies itself into a larger program modifying that program. Executes when a host program begins to run. Replicates itself, infecting other programs as it reproduces. Degrades system performance, destroys data.



TRAP DOOR: A mechanism built into a system by the designer. Function, enable designer to sneak back into system.



LOGIC BOMB: A type of trojan horse. Used to release a virus, a worm, or other system attacker. Triggers unauthorized action when a particular date, time or condition occurs.



TROJAN HORSE: A code or fragment that hides inside a program and performs a disguised function.



RABBIT: A rapidly reproducing computer program, usually containing a malicious code.

Follow computer security guidelines: adversaries preferred to go after easy targets. Keep your computer security up-to-date and make yourself a hard target.

Treat links and files carefully: social engineers and hackers post links in comments and try to trick you into downloading an "upgrade," "security patch," or "game."

Keep your passwords secure: use different, strong passwords for each online account. Never give your password away.

Do not depend on the SNS for confidentiality: even SNSs that aren't open and public by design can become so due to hacking, security errors, poor data management practices, and data brokering. In some cases, the site terms of service explicitly claim ownership of all your posted content.

Do not trust add-ons: plug-ins, games, and applications are often written by other users, not the SNSs themselves. The authors can easily gain access to your data once you install them.

Reviewer your friend's profiles: the photos or information they post about you may be a problem.