Operations Security

OPSEC

And Internet Safety

Do you have a web log (blog), personal or family web page, or use instant messaging? If so, realize there can be risks associated with using these forms of media.

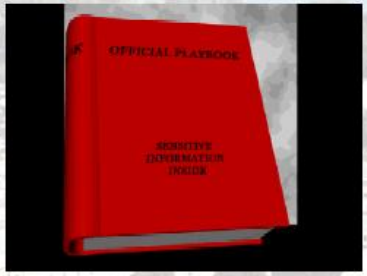
IS THERE REALLY A RISK?

Estimates show that approximately 900 MILLION people have Internet access. Realize not everyone on the Internet is a patriotic American. If you are going to post information out on the worldwide web consider the audience – 900 Million people! Some people use the Internet for disreputable purposes to engage in illegal practices such as identity theft, or even worse, use social engineering tactics to exploit you or your family.

If you are going to use blogs, personal web pages or instant messaging, be sure to keep safety in mind while doing so. Additionally be careful not to divulge sensitive DoD information – information that by nature of your association with DoD the general public would not have access.

OPSEC FOR DOD PERSONNEL

If you are a DoD employee, remember information you have access to – even though unclassified, can be valuable to adversaries.



Be careful not to post sensitive information about DoD activities on your blog or web page. Also take caution about the pictures you post on the Internet from your work environment. These can be valuable to our adversaries so don't help them conduct surveillance by posting photos of DoD facilities.

- If you are not sure if the information you wish to post is DoD sensitive information – ask your supervisor, or your security or OPSEC manager
- In many DoD facilities photography is prohibited. Make sure the pictures you wish to post do not violate DoD policy
- Be courteous when posting information about colleagues and co-workers. Be sure to respect their right to privacy especially when giving names and posting photographs
- While there are no restrictions on what you can say about yourself, there is a fine line between what you can say about DoD personnel and information. Be careful not to divulge official DoD information
- Remember, just because DoD information may be unclassified, doesn't mean it's appropriate for the worldwide web.

OPSEC FOR FAMILY MEMBERS

OPSEC is a method DoD uses in order to identify and protect sensitive information. We do this by looking at ourselves from the "bad guys" perspective and then limit the details an adversary would find useful. It's the same as using street smarts.

Think about what the bad guy would want to know - then take measures to protect yourself.

Family members play a key role in OPSEC! As family members you may have access to sensitive information. It's very important you be aware of the risks when posting information - even indirectly related to DoD activities on the Internet. Not only is it important to protect your DoD family member, but others in your household as well. You can help keep your family safe by:

- Not posting information about upcoming deployments or TDYs
- Not giving details about what kind of work your DoD family member performs for the military or government
- If your family member is deployed in support of a military operation, don't give details about the location or the activities your family member is involved in. Terrorists could be viewing your blogs and web pages!
- Realize that even if you install security protocols or password protection on your blog or personal web page – they're not fool proof!
- Refrain from posting specific identifying information such as your phone number and address
- Don't provide information that would allow someone to find you or your family. Writing about the school your child attends along pictures of your children are potential clues to help predators locate you or your family
- Don't post your email address on your page. Small town Internet host providers and personal information contained in your email address can be another clue. Rangerskid@smalltownisp.com

Realize the bad guys (terrorists, spies, and criminals) are out there just waiting to take advantage of others. Help keep your family safe by using OPSEC.

INTERNET SAFETY REMINDERS

Here are a few tips to consider when posting information accessible to the worldwide web:

- Think before you post - once it's out there it's gone!
- Don't post inappropriate or embarrassing information about yourself or others
- Use caution when posting photographs
- Establish security protocols on your blog or web page such as encryption or password protection. However, realize – these are not fool proof
- If you don't want the information to wind up in the Washington Post – then don't put it on your site
- If you don't want Al'Qaida to know where you or your family member is deploying to and what goes on there – than don't post it on your site

- If you are going to speak about your role in DoD make sure to state that your views do not necessarily reflect those of DoD

Realize criminals use the Internet too. Don't post information about yourself or your family members that would increase the risk of identity theft or other forms of exploitation. And remember to use caution when posting information about DoD activities.

TeamBliss
"Serving the Nation"