NAVY INFORMATION
OPERATIONS COMMAND
NORFOLK

OPSEC and SOCIAL NETWORKING SITES (SNS)

Social networking sites (SNS) allow people to collaborate and connect to share information and ideas. Essentially, these sites allow an individual to socialize in cyberspace.

There are a multitude of sites tailored to government employees, specific professions (firefighting, law enforcement, etc), and the military. Typically, these sites offer the ability for one person to post a comment and others to respond and have a conversation.

Do's to Consider

Do... find out who owns the SNS? Where are they hosted? Who has access to the data?

Do... optimize the use of Profile AND Search Controls. Often times these two functions operate independent from one another.

Do... verify "friend requests" before adding them to your profile.

Do... talk with your "friends" about sharing the information posted on your profile. Are they sharing any information you want kept private?

Do... become familiar with data aggregation. Every piece of data you supply online is collected or has the potential for collection by companies willing to buy, sell, and trade your data with others. Over time, this creates a complete profile of you and everything you do. Never post information that you would not share with a complete stranger.

Do... assume what you write on a social networking site is permanent. Even if you have the ability to delete your account, anyone on the Internet can easily print out the information, save it to a computer, or retrieve it from an archive site.

Don'ts to Consider

Don't... post sensitive information. Almost all SNS have vulnerabilities and security issues that make it possible, and probable, that the information posted on your profile will be more widely spread than you intended.

Don't... use the same logins and passwords for multiple websites. (SNS and banking)

Don't... trust add-ons, plug-ins, games, or applications. These are not created by the SNS, they merely host them for a fee from a third-party provider.

Don't... provide all friends with the same level of permissions. Create user groups with specific rules for access to and editing of photos, postings, and walls.

Don't... post personal information about yourself such as addresses, phone numbers, schedules etc...Your friends should already have this information, imposters don't!

Don't... post anything you wouldn't be comfortable with if it were to become public knowledge.

Kids on the Internet

Teach your children about cyber bullying. As soon as your children are old enough to use social web sites, talk with them about cyber bullying. Let them know that if they think they are being cyber bullied or harassed, they should share this information right away with a parent, a teacher, or an adult they trust.

Be smart about details in photographs. Explain to your children that photographs can reveal a lot of information. Encourage your children not to post photographs of high value items such as computers and electronic equipment or something that may clearly identify personnel information.

Set your own house Internet rules. As soon as your children begin to use the Internet, it is a good idea to come up with a list of rules everyone can agree on. These rules should include whether your children can have use of social web sites.

Ensure your children follow age limits on the site. The recommended age for signing up for social web sites is usually 13 and over. If your children are under the recommended age for these sites, ensure you monitor their activity. It is important to remember that you cannot rely on the site's services to keep your underage children from signing up.

Educate yourself about the site. Evaluate the sites your children plan to use and make sure both you and your children understand the privacy policy and the code of conduct. Find out if the site monitors content that users post. Also, periodically review your children's page.

Insist your children never meet anyone in person they have communicated with only online. Encourage them to communicate with people they already know. It might not be enough to simply tell your child not to talk to strangers — your child might not consider someone they have "met" online to be a stranger.

Be wary of other identifiable information in your children profile. Many social web sites allow children to join public groups, for example everyone who goes to a certain school.

Be aware when your children reveal information that could be used to identify them, such as school mascots, their workplace, or the name of the town they live in. Too much information can make your children vulnerable to cyber bullying, internet predators, internet fraud, or identity theft.

Warn your children about expressing emotions to strangers. You have probably already encouraged your children not to communicate with strangers directly online. However, children use social web sites to write journals and poems that often express strong emotions. Explain to your children that anyone with access to the internet can read what they post and that predators often search out emotionally vulnerable children.

NAVY INFORMATION OPERATIONS
COMMAND NORFOLK (NIOC)
Norfolk 757.417.7100
San Diego 619.545.4588
Email: opsec@navy.mil