



THE UNITED STATES AIR FORCE SAP SECURITY BULLETIN



PUBLISHED BY THE
SPECIAL PROGRAM SECURITY EDUCATION & PROFESSIONALIZATION BRANCH

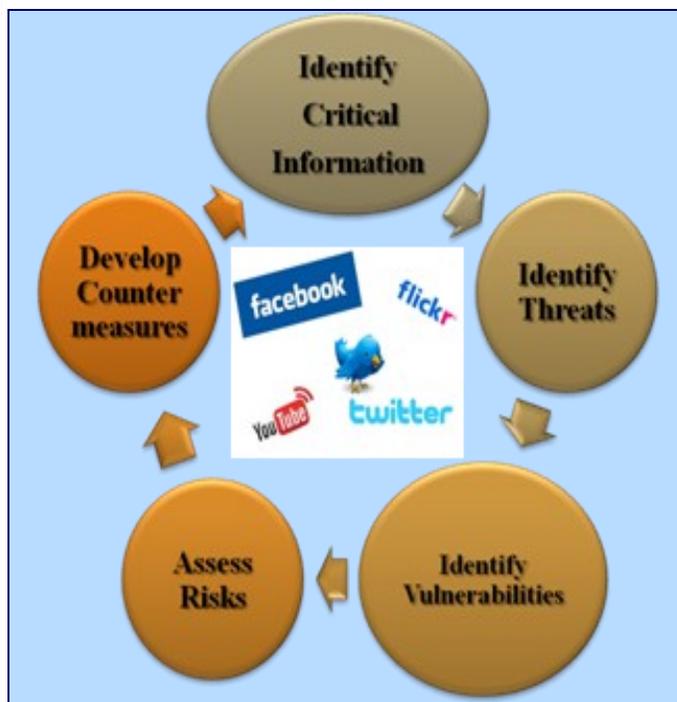
SAF/AAZ
1720 Air Force Pentagon
Washington, DC 20330-1720

1 December 2011

Volume 2, Issue 4

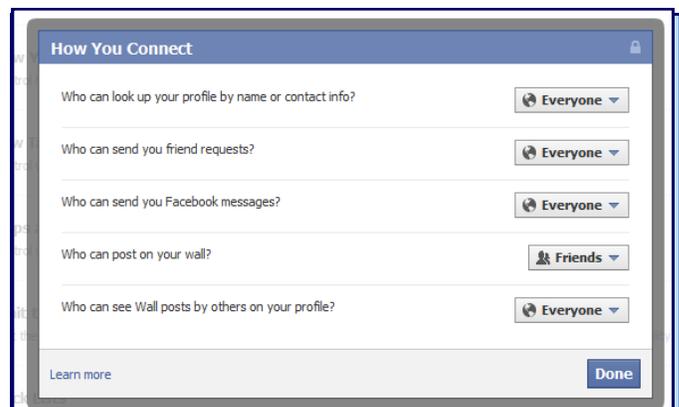
APPLYING OPSEC TO SOCIAL NETWORKING

Social networking sites (SNS) are used by millions of individuals on a daily basis, and like it or not, they have become ingrained in our society. While most of us use these sites to connect with the people we know, there are those that use them to gain information they wouldn't otherwise have access to, and at our expense. Accessibility and ease of use make it especially important for DoD personnel and their families to understand the risks involved and take steps to protect themselves. By applying the fundamentals of Operations Security (OPSEC), we can identify what information should be protected, and from whom. OPSEC is a methodology that denies critical information to an adversary.



The first step in this process is indentifying the types of information that adversaries use to their advantage. When applied to social networking, two types of information that require protection are work related information and personal information.

Work related information encompasses your title or position, duty location, the agency you work for, and any specific information related to the work you do on a day to day basis. Personal information includes your name, address, the members of your family, and any of your contact information or financial details. Personal information also applies to your daily activity, which adversaries can use to verify what you are doing, where you are, or where you aren't at any given time.



Here we see an example of weak social networking security.

Information requires protection in large part because of the threats to it. Due to the nature of the work we do, and who it's for, serious threats to work related information include foreign intelligence services and enemies of the United States. A TDY location or

KEEP YOURSELF SAFE ON-LINE

project you're currently working on is routine information to you, but to the enemy, it's useful data that they couldn't attain by other means.

Hackers and cyber-criminals look to exploit the deficiencies of technological systems for personal gain. By using all available security measures on SNS, we reduce the risk and likelihood that we will be targeted by these threats. An additional threat to consider is the criminal who is always looking for a target of opportunity.

Someone who comes back from a vacation to find their house broken into and their property stolen might find that their tweet or post about how long they'd be away was not the best idea.

Following the five-step OPSEC process then brings us to identifying vulnerabilities. While we make ourselves vulnerable by sharing information we should protect, there are other vulnerabilities inherent to internet use and computer programs. On sites like Twitter and Facebook, when you look at the address in the web browser, you will likely see "http://", which indicates the connection between the web browser and the site you are on is unsecure, and can be viewed by someone else.

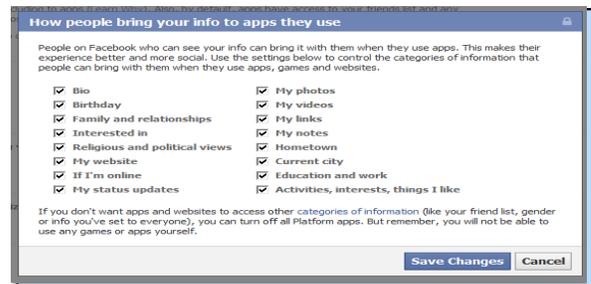
When using these sites, and especially when providing any personal (social security number) or financial (bank account, credit card numbers) information, ensure that the web address has a secure connection, signified by "https://". Many times, such as on Facebook, this extra security measure must be enacted manually in the "settings" section, as the site will opt-out of this setting rather than opt-in. Because of this, your profile security must also be set manually.



Profile security also includes what information you provide, as it is often the first thing seen when searching a SNS. The search function is often used to find other people with similar backgrounds and interests as yours, and while this is a useful tool to network and build camaraderie, it could also identify your affiliations, work location, or unit.

Third party applications like "Mafia Wars" and "Farmville" also share your personal information with others unless you manually restrict their access. In the example below, a large amount of personal information is being shared with third party apps. Since you don't know who created these applications, think of it as walking up to a stranger on the street and giving them your name, birth date, address, and contact information.

Some of the risks associated with sharing information on SNS are personal loss (identity, information, property or money) and being subject to influence from foreign entities. Disciplinary action or termination at your job could also result from sharing work related information on the internet, so take steps to protect yourself from these risks.



Effective countermeasures should be considered to help increase your level of information protection. Use social networking to maintain existing relationships as opposed to creating new ones. Take the time and effort to personally enable the most stringent security settings these websites offer, and use private messages to communicate with specific individuals. Above all, be mindful of what information you share so that you can continue to connect with the right people, and keep the wrong people from connecting with you.