Counterintelligence and Social Networking

San Diego ISAC Counterintelligence Sub-Committee - April 2016

SOCIAL NETWORKING – USEFUL AND IMPORTANT, BUT….
There is no doubt social networking sites are an extremely useful and important tool, with a multitude of uses. For the purposes of this article we will categorize social networking sites two-fold: 1) the social-personal site which enables one to keep in touch with family and friends while expanding one's social circle, and 2) the social-professional site which aides one along in his/her career. In most cases the social-professional site gets more attention at the workplace, especially as the professional world becomes more and more competitive. For those of us who have recently faced the challenges of the current job market it is recognized most employers will not consider a candidate without a mature social networking profile. Unfortunately, the extensive amount of information maintained on these websites, both personal and professional, have led to the sites being a potential gold mine for individuals who are looking for ways to acquire sensitive information.

COUNTERINTELLIGENCE AND REPORTING REQUIREMENTS
While the National Industrial Security Program Operating Manual and supplemental Industrial Security Letters call out the requirement for cleared employees to be aware of reporting suspicious contacts to the Facility Security Officer (FSO), it is necessary to cite the specific:

> NISPOM 1-302b. Suspicious Contacts. "Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to

> classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported."

ADVERSARIES USE SOCIAL NETWORKS?

In the not-too-distant past, the co-founder of a dating service and social dynamics instructional course decided to perform a case study after hearing some clients, who happened to be scientists with personnel security clearances, discussing some of their work projects under development. Within the framework of the case study a fake social-professional networking account was created reflecting a recruiter profile with an image of an attractive female. While online, several of the cleared individuals openly discussed personal details about themselves as well as work matters related to the projects under development without regard to the fact disclosures were being made to a complete stranger.

The case study was developed further with the same image being used on a popular social-personal networking site; in this scenario the profile of a professional recruiter was changed to that of an aspiring young engineer. Many of the scientists who were hesitant to engage in discussion and reveal details on the social-professional networking site changed tune and openly discussed matters on the social-personal networking site.

Findings of the case study were published at a security conference. Of particular interest was the identification of Trust Triggers, which are strategies used by collectors to get targets to open up, build comfort and confidence, and potentially gather sensitive information. Common Trust Triggers used in social networks are

- Revealing a personal detail to another in order to get the other to reveal information he or she normally would not, almost a tit for tat wherein the other feels both trust and an obligation to engage personally; and
- Asking for help and appearing vulnerable; oftentimes individuals will look past a violation of privacy or security if there is an opportunity to help someone in need.

It is useful to recognize information which is not revealed in certain environmental contexts and groups may often be revealed elsewhere, what may be revealed on a social-personal site may be found on a social-professional site and vice versa. With this possibility it is especially important to remain consistent and vigilant regarding the protection of both work and personal information.

HOW DO WE COUNTER POTENTIALLY OFFENSIVE EFFORTS?

It is a very thin line we walk in social networking. There is both a want and a need to be as personable and impressive as possible without revealing sensitive information. It is also important to keep in mind that it does not take a lot of information to become too much, or to be cognizant of the fact the collector with purpose will be able to gather bits and pieces of information across any wide array of social networking sites towards better understanding the whole.

The following are some of things to think about regarding creating and maintaining any number of accounts on social networking sites, whether professional or personal:

- Oversharing not only puts information at risk, but it also puts your account and personal interests at risk; for instance, touting a daughter's softball team and athletic feats, while having the password "Softball" is not advisable;
- Be consistent throughout all accounts regarding the information revealed; drawing boundary lines between a personal vice professional social networking account achieves nothing beyond giving the collector a better idea of preferences and supposed norms;
- Maximize and update your privacy settings to secure your profile and limit audience availability of information posted…on every type account used;
- Disable the GPS tracking feature on your phone – The cool picture of your family at the Washington Monument does not have to be uploaded immediately;
- Be wary of "Trust Triggers" – especially those persons who appear vulnerable or in need of help;
- Use a different password for each account maintained, as using one password makes for a weak and easy target;
- Unsolicited contacts, connections, and invitations from strangers are simply that, and the social connection of a mutual friend may need to be validated.

CONCLUSION – REMEMBER OPSEC ALL THE TIME

It is estimated upwards of 90 percent of the information intelligence collectors acquire come from unclassified sources, to include newspapers and periodicals, social media posts, tweets, text messages, and even online videos. With so much information available to everyone, by making even the simplest changes in an account security settings or being more conservative with how much information is revealed can make a big difference in reducing your chances of being targeted.

REMEMBER THE PREVIOUS CI ARTICLE? REPORT, REPORT, REPORT

Finally, be sure fellow employees are aware of the kinds of information gathering methods that have previously been used, and then encourage all to take the next step of reporting any unusual exchanges on social networking sites. The importance of understanding a threat cannot be minimized. Proper safeguards cannot be effective without the full understanding the adversary and their methods, and this is why it is so important to report ANY suspicious activity to the local FSO. In fact, you may find it a worthwhile effort of your own to create or use an existing account to simply search your own workplace and/or programs supported. You may be surprised at seeing who fellow employees are connected with or what fellow employees are providing updates on.