

Cyber/Social Networking: Things You Need to Consider

Florida Research Administration Conference

January 16th 2015

Dela Williams
Facility Security Officer



UNIVERSITY OF CENTRAL FLORIDA

Agenda

- ❖ Overview
- ❖ Privacy and Records
 - ❖ Policies and Procedures
- ❖ Personal Risks and Mitigations
- ❖ Technical Risks and Mitigations
- ❖ Cyber-crime and Mitigation Efforts
- ❖ Cyber-espionage and Mitigation Efforts
- ❖ Impact to Defense Industry
- ❖ Summary

Privacy and Records

- ❖ Challenges to be addressed
 - ❖ Federal Agencies (DoD, DHS, etc.) are using social networking sites to better connect with the public.
 - ❖ What on these sites now becomes information owned by the government?
 - ❖ How do these sites fit into the policies of the Freedom of Information Act, the Paperwork Reduction Act, and the Privacy Act?



Policies and Procedures

- ❖ Government agencies, such as the National Archives and Records Administration (NARA), DHS, the General Services Administration, and the Office of Management and Budget have each issued guidelines.
 - ❖ NARA on what constitutes an “official record”
 - ❖ DHS on the use of social media to promote the President’s Transparency and Open Government Initiative
 - ❖ GSA on terms of service agreements with social networking providers
 - ❖ OMB on how the PRA and Privacy Acts apply to information on government use of third party web sites and applications.



DoD Policies

Agencies and Departments setting foundational Social Media policy to establish governance processes and risk thresholds

CIO 2106.1 GSA Social Media Policy

Date: 07/17/2009
Status.: Validated
Outdated on: 07/17/2019

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

GSA ORDER

SUBJECT: GSA Social Media Policy

1. Purpose. This Order establishes policy for employee use of social media.
2. Applicability. This Order applies to all GSA employees. It also applies to contractors on behalf of GSA as part of their duties.
3. Background. GSA encourages the use of social media technologies to enhance information exchange in support of GSA's mission. By openly sharing knowledge within the agency, with and from other federal, state, and local partners, and we provide more effective solutions and efficiencies to enhance excellence in the business.
4. Definitions. "Social media" and "Web 2.0" are umbrella terms that encompass technology, social interaction, and content creation. Social media use many techniques, including photo and video sharing, podcasts, social networking, mashups, and virtual Social Media defines these and other tools.
5. Guiding Principles.



NAVY COMMAND SOCIAL MEDIA HANDBOOK



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office Chief Information Officer (IG)

15 2010

SAIS-GKM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Responsible Use of Internet-based Capabilities

1. References:

- a. Directive-Type Memorandum 09-026, Responsible and Effective Use of Internet based Capabilities, 25 February 2010.
 - b. CIOIG-6 Memorandum, Use of Social Media Tools, 27 August 2009.
2. This memorandum provides updated guidance to the Army regarding the use of Internet-based Capabilities, and is based on policy released by the Deputy Secretary of Defense (reference a). This policy supersedes prior social media guidance released in August 2009 (reference b).
 3. Per DoD policy, the NIPRNET shall be configured to provide access to Internet-based capabilities across all DoD components. Commanders at all levels must continue to defend against malicious activity affecting Army networks. They therefore may take actions to limit access to Internet-based capabilities on a temporary basis in order to ensure that a mission is safeguarded or to preserve operations security.
 4. Social media sites are often deployed in an environment that is not under the Army's direct control. Commanders, Soldiers and civilians affiliated with the Army must follow the requirements outlined in the enclosures to ensure that Army networks are protected and that operations security is maintained.
 5. The point of contact for this memorandum is Ms. Amber Pittser; she can be reached at amber.pittser@us.army.mil or 703-602-0274.



Fall 2010

The Dark Side of Social Networks

Personal data of 170 million Facebook users exposed, collected, and shared without any hacking

By [Ed Oswald](#) | Published July 29, 2010, 5:40 PM

[Print Article](#)

[E-mail Article](#)

[75 Comments](#)

Using publicly available information on Facebook, a researcher has been able to gather personal details of nearly 170 million users of the service, or about a third of all users. The data includes names, addresses, e-mails, phone numbers, and birthdays: essentially anything that was not marked as private is now part of this file.

The file has now ended up on The Pirate Bay, and so far has seen over 10,000 downloads. This could mean hackers would have an easy way to obtain personal information necessary for identity theft and other malicious uses.

People who are using Facebook either do not care about protecting their information or do not know how. This is a systemic problem across the majority of Social Media platforms

<http://www.betanews.com/article/Personal-data-of-170-million-Facebook-users-exposed-collected-and-shared-without-any-hacking/1280439164>

The Dark Side of Social Networks



Did you know?

- ❖ A U.S. 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.
- ❖ New computer viruses and Trojans that successfully target information on social networking sites are on the rise.
- ❖ Information on social networking sites has led to people losing job offers, getting fired and even being arrested.
- ❖ Social networking sites have become a haven for identity thieves and con artists trying to use your information against you.
- ❖ Several kidnapping, rape and murder cases were linked to social networking sites where the victims first connected with their attackers.
- ❖ According to the Al Qaeda Handbook, terrorists search online for data about “Government personnel and all matters related to them (residence, work place, times of leaving and returning, children and places visited.)”

Source: Interagency OPSEC Support Staff

Personal Risks

- ❖ “Facebook fired”
 - ❖ Venting about co-workers/boss
 - ❖ HR considerations
- ❖ Company reputation
 - ❖ Whether good or bad, needs to left to the “professionals” (Public Affairs)
- ❖ Social Engineering
 - ❖ Financial Officers
 - ❖ Government Employees
- ❖ Geotagging
- ❖ Location based Social Networking



Privacy Settings

- ❖ Understanding what you can and cannot post on social media platforms goes a long way in protecting yourself online, but more can be done by adjusting your privacy settings on social media sites.
- ❖ Facebook's default privacy settings are often public, but Facebook provides various setting options that help Facebook users adjust privacy settings.
- ❖ Twitter allows users to keep their Tweets private and Flickr gives users the option of keeping photos private. The settings are easily accessible, the trick is setting them to meet your privacy needs. Similar privacy settings can be found on other social media sites like Myspace and LinkedIn.

Facebook

Everyone	Everyone	Friends of Friends	Friends Only	Other
Friends of Friends	Your status, photos, and posts	*		
Friends Only	Bio and favorite quotations	*		
Recommended	Family and relationships	*		
Custom	Photos and videos you're tagged in	*		
	Religious and political views	*		
	Birthday	*		
	Permission to comment on your posts		*	
	Places you check in to [?]		*	
	Contact information		*	
	<input checked="" type="checkbox"/> Share a tagged post with friends of the friend I tag			

Sharing on Facebook

Everyone	Everyone	Friends of Friends	Friends Only	Other
Friends of Friends	My status, photos, and posts	*		
Friends Only	Bio and favorite quotations	*		
	Family and relationships	*		
Recommended	Photos and videos I'm tagged in			*
Custom	Religious and political views			*
	Birthday		*	
	Can comment on posts		*	
	Places I check in to [?]		*	
	Contact information			*

Twitter

Tweet Privacy Protect my tweets

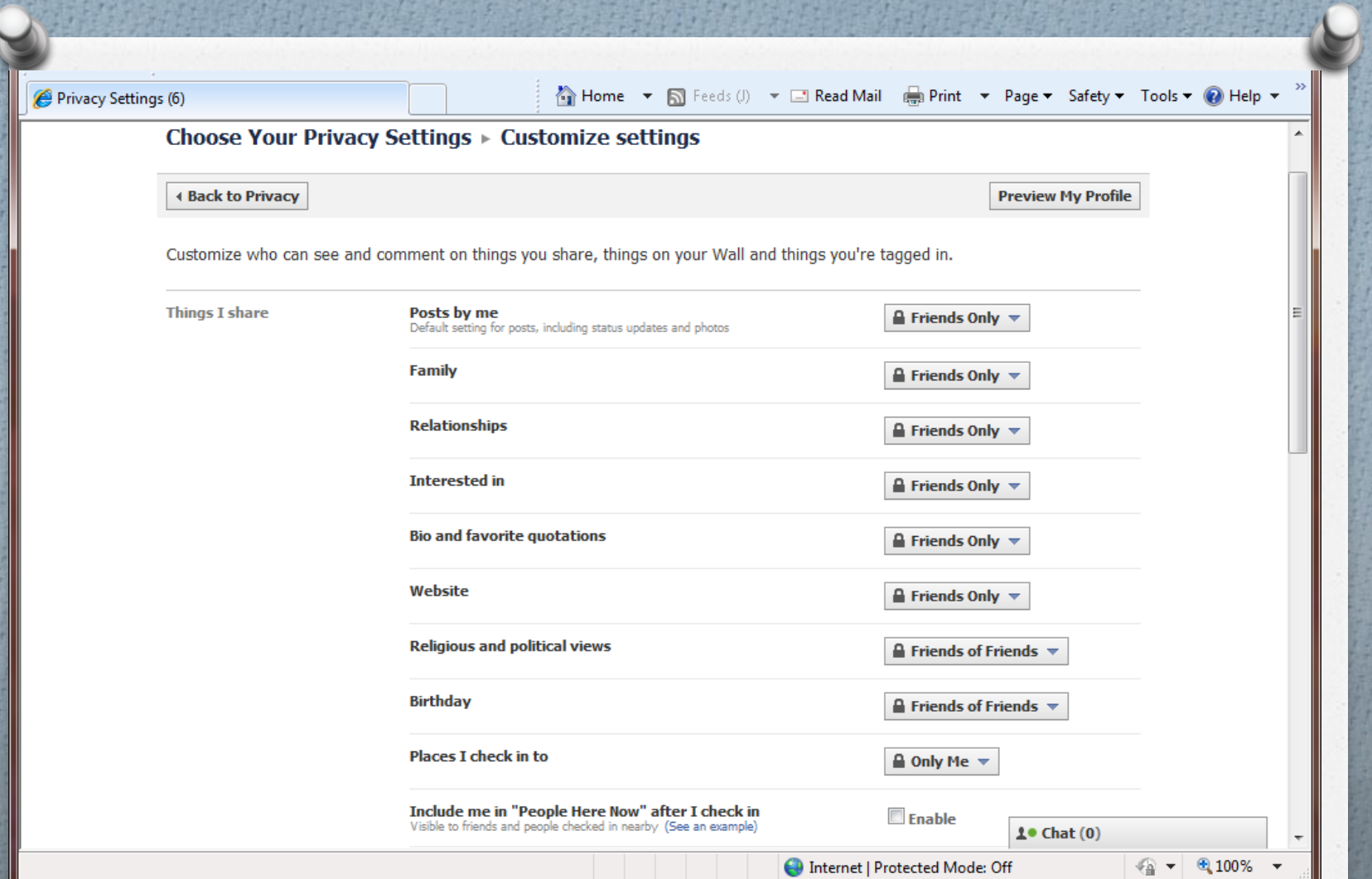
Only let people whom I approve follow my tweets.

If this is checked, your future tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places.

Facebook Privacy Settings

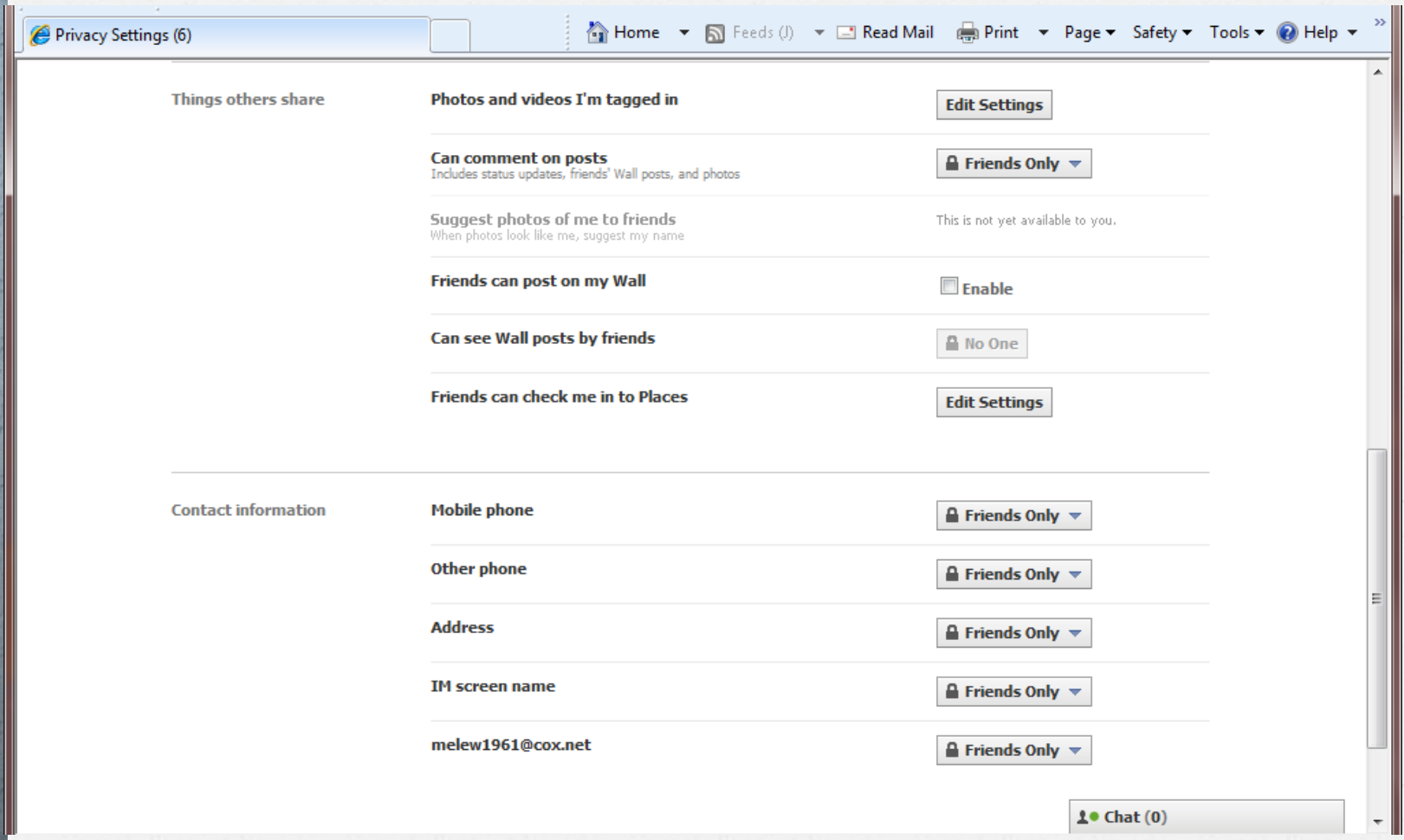
- ❖ Click on “account”
- ❖ Click on “privacy settings”
- ❖ Under “Things I share” disable “People here and now after I check in” by un-checking the box.
- ❖ Also under “Things I share” change the “Places I check into” to “only me” by customizing the setting.



A screenshot of a web browser displaying the Facebook Privacy Settings page. The browser's address bar shows "Privacy Settings (6)". The navigation bar includes links for Home, Feeds, Read Mail, Print, Page, Safety, Tools, and Help. The main heading is "Choose Your Privacy Settings" with a sub-heading "Customize settings". Below this are two buttons: "Back to Privacy" and "Preview My Profile". A descriptive text states: "Customize who can see and comment on things you share, things on your Wall and things you're tagged in." The settings are organized under the heading "Things I share". Each item has a category name, a brief description, and a privacy dropdown menu. The items and their settings are: "Posts by me" (Default setting for posts, including status updates and photos) set to "Friends Only"; "Family" set to "Friends Only"; "Relationships" set to "Friends Only"; "Interested in" set to "Friends Only"; "Bio and favorite quotations" set to "Friends Only"; "Website" set to "Friends Only"; "Religious and political views" set to "Friends of Friends"; "Birthday" set to "Friends of Friends"; "Places I check in to" set to "Only Me"; and "Include me in 'People Here Now' after I check in" (Visible to friends and people checked in nearby) with an "Enable" checkbox. A "Chat (0)" button is visible at the bottom right. The browser's status bar at the bottom shows "Internet | Protected Mode: Off" and a zoom level of "100%".

As you can see, there are many other things you can customize to protect your information

Even more options to customize to protect your information.



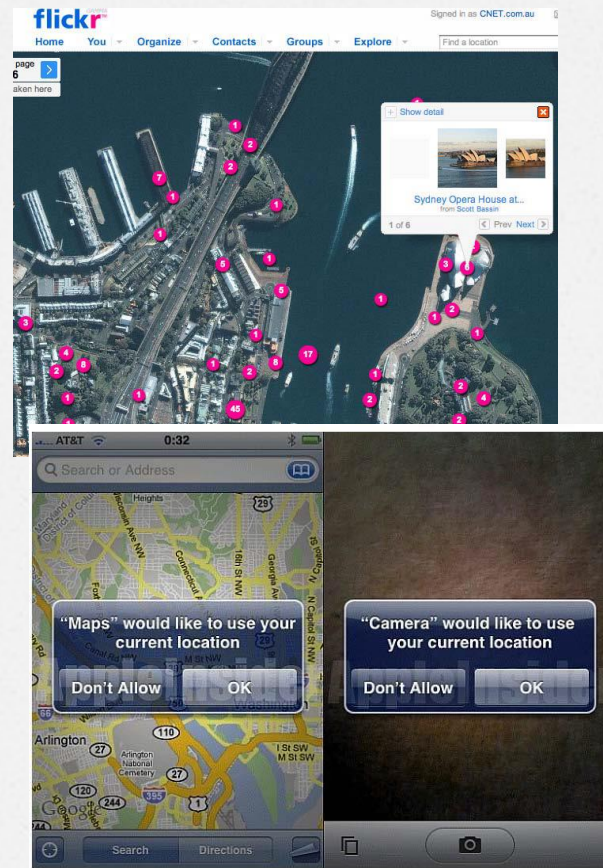
The screenshot shows the Facebook Privacy Settings interface. At the top, there is a navigation bar with links for Home, Feeds, Read Mail, Print, Page, Safety, Tools, and Help. The main content is divided into two sections: 'Things others share' and 'Contact information'. Each section contains several settings with corresponding controls like 'Edit Settings' buttons and dropdown menus.

Section	Setting	Control
Things others share	Photos and videos I'm tagged in	Edit Settings
	Can comment on posts <small>Includes status updates, friends' Wall posts, and photos</small>	Friends Only
	Suggest photos of me to friends <small>When photos look like me, suggest my name</small>	This is not yet available to you.
	Friends can post on my Wall	Enable
	Can see Wall posts by friends	No One
	Friends can check me in to Places	Edit Settings
Contact information	Mobile phone	Friends Only
	Other phone	Friends Only
	Address	Friends Only
	IM screen name	Friends Only
	melew1961@cox.net	Friends Only

Chat (0)

Geotagging Safety

- ❖ Geotagging is the process of adding geographical identification to photographs, video, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything you post on the internet.
- ❖ Geotags are automatically embedded in some pictures taken with smartphones. Many people are unaware of the fact that the photos they take with their smartphones and load to the Internet have been geotagged.
- ❖ Photos posted to photo sharing sites like Flickr and Picasa can also be tagged with location, but it is not an automatic function.



Geotagging Safety

- ❖ Location-based social networking is quickly growing in popularity. A variety of applications are capitalizing on users' desire to broadcast their geographic location.
- ❖ The increased popularity of these applications is changing the way we as a digital culture view security and privacy on an individual level.



Personal Mitigation Efforts

- ❖ Be careful what you post on your social networking sites
- ❖ Refer all inquiries about your company to the appropriate office (public affairs, legal, HR)
- ❖ Keep your personal information secure. Check security settings on social networking sites regularly to be sure they are still in effect.
- ❖ Check your devices to be sure that if you do not want people to know your every move, you are not inadvertently broadcasting that information.

Technical Threats

❖ Malware

- ❖ According to the managing director for RSA “the leading infection method (for malware) are drive-by downloads, which hijack legitimate web sites and route visitors to infected servers”.



❖ Spam

- ❖ This method can also be used to direct users to infected servers through social networking sites.

❖ Phishing/Spear Phishing

- ❖ Attempts to get personally identifiable information (PII) in order to get access to computers, bank accounts and credit card information.



Technical Mitigation Efforts

- ❖ Keep software/virus patches up to date
- ❖ Have strong auditing policies in place
- ❖ Have strong password policies in place
- ❖ Use authentication software to protect identity from “spoofing”
- ❖ Report suspicious emails or contacts to security



Cyber-Crime

- ❖ Phishing efforts are more likely to succeed if there are large numbers of potential victims.
- ❖ Criminals use “trust” built into social networking sites to lead victims to malicious web sites and servers.



Data Collection and Uses

- ❖ Social media platforms collect information that includes typical profile information, hobbies, interests, network address purposes other than enhancing the user experience.
 - ❖ This collected information can be used for purposes other than what was intended or expected by the user of the social media platform.
 - ❖ Third parties can create a digital dossier of personal data that can be used by an adversary to embarrass, blackmail or damage the image of a profile holder.

Cyber-Crime Mitigation Efforts

- ❖ Social networking companies are working with law enforcement to detect and prosecute criminals.
- ❖ Educating users on site security policies
- ❖ Introducing software that can track and stop attacks on social networking sites
- ❖ Legal challenges to be overcome include jurisdictional considerations and legal definitions of privacy.



Cyber-Espionage

- ❖ Social Engineering through malicious emails remains the #1 method of operation.
 - ❖ Sites like LinkedIn give attackers additional means to find out more about a person's business relationships
- ❖ Looking for new exploitation methods through compromising home systems and social networking sites of DoD and cleared contractors.



Social Engineering Attacks

- ❖ Signs of a Social Engineering attack
 - ❖ Refusal to give contact information
 - ❖ Rushing
 - ❖ Name-dropping
 - ❖ Intimidation
 - ❖ Spelling errors, wrong name, odd questions
 - ❖ Request for forbidden information

Impact to Defense Industry

- ❖ Stolen unclassified DoD/U.S. Government data aids adversary:
 - ❖ Strategically, operational, tactically
 - ❖ More compromised accounts leads to a stronger adversary foothold in network
 - ❖ Advance their research and development programs
- ❖ Potential loss of confidence in data
- ❖ Loss of availability of data and network connectivity
- ❖ Cost of remediation



Summary: Using Social Networks in the Office

- ❖ Consider restricting access to these sites or limit access to only certain sites.
- ❖ Establish policies for creating, maintaining and destroying social media accounts
- ❖ Establish “Acceptable Use Policies” about how and when to use social networks
- ❖ Establish policies for content management
- ❖ Prepare for risks of allowing the use of social networks
- ❖ Legal issues may require a disclaimer for use by employees as well as attention to laws regarding data retention and transactional auditing

Summary: Using Social Networks for Families

Security items to consider

- ❖ Take a close look at all privacy settings. Set security options to allow visibility to “friends only.”
- ❖ Do not reveal sensitive information about yourself such as schedules and event locations.
- ❖ Ask, “What could the wrong person do with this information?” and “Could it compromise the safety of myself or my family?”
- ❖ Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone.
- ❖ Closely review photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released.
- ❖ Make sure to talk to family about operations security and what can and cannot be posted.
- ❖ Videos can go viral quickly, make sure they don’t give away sensitive information.

Summary: Using Social Networks for Families

Social media concerns for children

- ❖ What is the best way to protect your kids online? Talk to them. Research suggests that when children want important information, most rely on their parents.
- ❖ The important thing is to start the education early. Talk to your children about online risks and make sure you create an honest and open environment.
- ❖ Some social media sites like Facebook, provide family safety resources and tools for reporting issues.

Summary: Countermeasures

These tips will help you protect critical information while using social media

- ❖ **Follow computer security guidelines:** Adversaries prefer to go after easy targets. Keep your computer security up-to-date and make yourself a hard target.
- ❖ **Never login from risky locations:** Public social networking sites generally do not have secure login available. If you login from a hotel, cyber-café or an airport hotspot, particularly ones in foreign countries, your name and password can be captured at any time.
- ❖ **Modify your search profile:** Do a search for yourself and if too much data comes up, you should consider adjusting your settings.
- ❖ **Keep your password secure:** Use different, strong passwords for each online account. Never give your password away.
- ❖ **Don't depend on the social media site for confidentiality:** Even social media sites that aren't open and public by design can become so due to hacking, security errors and poor data management practices. In some cases, the site terms of service explicitly claim ownership of all your posted content.
- ❖ **Treat links and files carefully:** Social engineers and hackers post links in comments and try to trick you into downloading an "update," "security patch" or "game."

Questions?

Dela Williams

Facility Security Officer

delawilliams@ucf.edu

407.882.1123



UNIVERSITY OF CENTRAL FLORIDA