SOCIAL MEDIA

Module 6

This module explore the theories and principles behind all of the mainstream social media venues, delve into the technical composition of the big social media platforms, explore the security risks associated with social media such as: the most common way hackers steal your information, how to steer clear of malware, spyware and virus threats, how to choose a password that's difficult to guess but easy to remember, how to set up two-factor authentication on Gmail, Facebook and Twitter and how to spot phishing and social engineering scams.

Key Concepts

- Risks of posting on personal vs. company social networking profiles
- What employers can prohibit employees from saying online
- Confidential information vs. what's okay to share
- Responsible on-duty vs. off-duty social networking conduct
- Personal privacy rights at work
- The rights employers have to monitor how their employees use social media
- Security and safety of your data

WHY USE SOCIAL MEDIA?

Personally

- Entertaining
- Maintain Relationships
- Network
- Centralized information

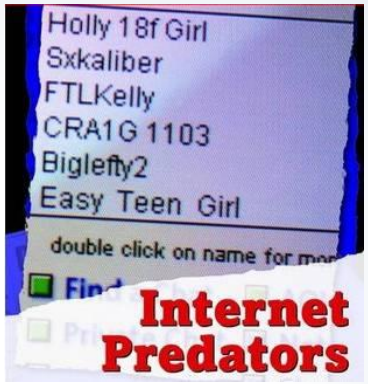
Professionally

- Marketing/recruiting
- Public Relations
- Connect with customers
- Solicit ideas and feedback

Social Networking Sites (SNS) allow people to network, interact and collaborate to share information, data and ideas without geographic boundaries.

Bad guys use it, too:

- Stalkers
- Thieves
- Terrorist
- Hackers
- Phishers/Scammers
- Enemy organizations
- Pedophiles
- And the list goes on…



Google Yourself!

You don't have to be on Facebook. Really. You don't. Social media isn't for everyone and if you don't feel comfortable sharing information online, don't feel forced because "everyone is doing it."

If you're not into networking online, you also probably won't be willing to take the time to safeguard your profiles, stay up with changes and trends, and follow the necessary steps to keep your privacy settings updated.

Know your settings

Did you know you can block your tweets so only individuals you approve can see what you post? Facebook offers a variety of privacy settings, and you can even choose individually who can see your photos. Take the time to secure your profiles so you're only sharing the information you choose.

Don't post personal information.

It should go without saying – keep the year of your birth, your address, your work email and other similar information personal, and don't display them, or use them to create, social media accounts.

Don't overshare.

This isn't just smart for security cleared professionals, we'd all save our friends a lot of groans if we refrained from sharing mundane, or scandalous details online. Oversharing isn't just annoying, it highlights you as a potential data mining or spear phishing victim.

Make sure your online friends are real friends.

Don't trust the information or profile picture – individuals you connect with online may not necessarily be who they say they are.

Don’t talk about work

Seems like a no-brainer if you work in intelligence, right? Be smart online, and don’t discuss the details of your job. The best way for security cleared professionals to use social media is to keep a distinction between the personal and professional.

Use a dedicated, secure network to connect professionally.

Social media is a powerful tool in your job search or career networking tool-kit. But sharing the details of your resume, job, or clearance level on searchable, public websites is risky. That's why the Cleared Network was created – it provides a secure, protected place to build your career network.

If you hold a security clearance or if you ever want to apply for one, be mindful of your postings and contacts online, particularly on social networking sites such as Facebook and Twitter. These sites pose risks to gaining and keeping a security clearance.

Question 14 of the National Agency Questionnaire (SF-86) asks for names of your relatives and associates. The term "associate" is defined as any foreign national that you or your spouse "are bound by affection, obligation, or close and continuing contact."

Social networking sites **bring a gray area** into the definition of an associate and continuing contact.

You may want to eliminate any foreign nationals from your social networking sites to eliminate any potential security concerns.

CONTROL YOUR SOCIAL MEDIA PRESENCE

Control your social media presence via self-restraint and the privacy settings on all of your social media accounts. The government has not officially said, ‘we are checking your social media presence,” but it is.

Any HR person who is hiring these days definitely does some Googling to check out job candidates, and security investigators do pull information from the social web.

- Social media has become a frequent place for spam and phishing attacks aimed at collecting confidential information.

- Twitter, Facebook, Instagram, Pinterest, and Tumblr include some of the often-targeted places. Here's the anatomy of one type of threat — suggesting you be careful what you click on in social media:

6 Ways You May Be Losing Mobile Data

And You Don't Even Know It

1

DEVICE LOSS AND THEFT
It's not the device that matters, but the potential link it provides to your company's applications and data.

2

DATA LEAKAGE
Well-intentioned employee actions, such as using the cloud for file sharing or collaboration, can lead to information exposure and attacks.

3

MALWARE AND MALICIOUS ATTACKS
The bad guys see mobility as their next target, while traditional IT isn't paying attention to mobile malware yet.

4

SHARED DEVICES AND PASSWORDS
Sharing accounts with friends and family causes most data breaches. Use two-factor authentication to protect business information.

5

JAILBREAKING AND ROOTING
Prevent user-modified devices from accessing the network, as they can circumvent important security features and policies.

6

WI-FI AND WIRELESS SNOOPING Discourage free Wi-Fi use. Companies have no control or visibility and these networks are prone to malicious traffic.

Social Networking Sites Online Friendships Can Mean Offline Peril

So what's the problem? These sites can be appealing to child sexual predators, too: all that easy and immediate access to information on potential victims. Even worse, kids want to look cool, so they sometimes post suggestive photos of themselves on the sites.

According to an Internet safety pamphlet recently published by NCMEC, a survey

- 12 to 17 year olds revealed that 38 percent had posted self-created content such as photos, videos, artwork, or stories.
- 10 to 17 year olds revealed 46 percent admit to having given out their personal information to someone they did not know.

The likelihood that kids will give out personal information over the Internet increases with age, with 56 percent of 16 to 17 year olds most likely sharing personal information.

- Protecting your computers may not be enough, either. Attacks on mobile devices continue to increase as the devices become more popular.
  - Symantec report identifies a **58 percent** increase in mobile malware from 2011 to 2012. Nearly **one-third** of those attacks also aim to steal information.

DON'T: DEPEND ON SOCIAL MEDIA'S SECURITY SETTINGS

But it's set to private … right?

- Hackers
- Incorrect or incomplete settings
- Sale of data
- Upgrades/site changes
- "Risks inherent in sharing information"

"USE AT YOUR OWN RISK.

We do not guarantee that only authorized persons will view your information."

Plugins, Games, Applications

- Third Party Software
- Applications designed to collect data
- Malicious code

- Separate terms of use & privacy
  - "We are not responsible for third party circumvention of any privacy settings or security measures."

DON'T: GRANT THE SAME ACCESS TO EVERYONE

Don't treat all Friends equally

Control & customize individual access

Do create groups

- Poker club
- Family

Set permissions for everything:

- Your status
- Photos
- Postings

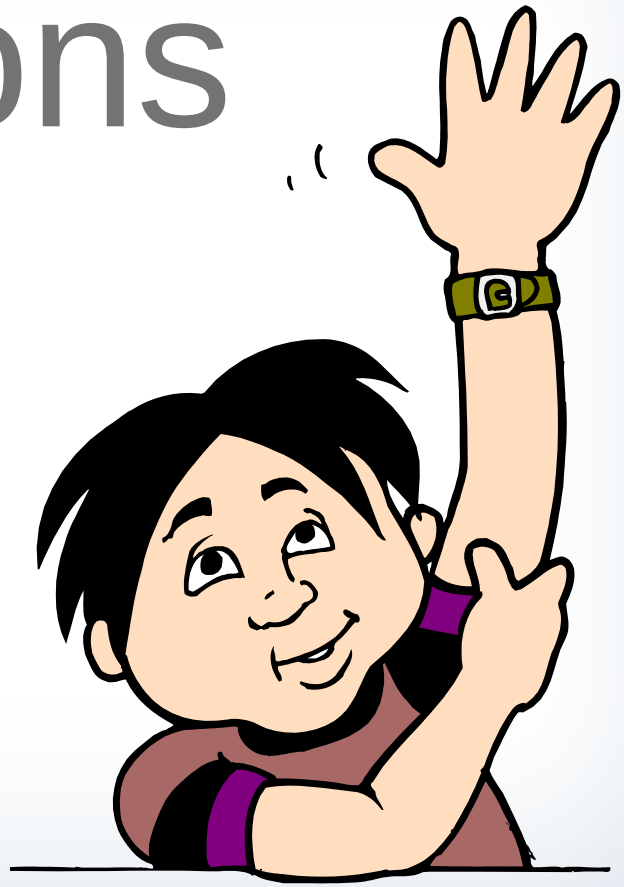
DETAILS MAKE YOU VULNERABLE

- Never post anything you would not tell directly to the enemy
- Never post private or personal information- no matter how secure you think your settings are
- Assume the information you share will be made public

ASSUME THE INTERNET IS FOREVER

- There is no true delete on the internet
- WWW means World Wide Web
- Every Picture
- Every Post
- Every Detail

Questions



Course Assessment Final Exam

Course Assessment Review of Final Exam

THANK YOU