Cyber Defense and Disaster Recovery Conference 2013: Mobile Security

7:30a	**Registration Check-in – Studio Theater Concourse, Public Affairs Center (PAC), 1st Floor** **Opening Remarks and Morning Plenary Session – Brookens Auditorium**		
8:15a	Opening Remarks – Brookens Auditorium Dr. Lynn Pardie – Vice Chancellor For Academic Affairs and Provost, University of Illinois Springfield David A. Ford – Special Agent in Charge, Federal Bureau of Investigation		
8:35a	Morning Plenary Session: Brookens Auditorium	**Mobile Device Threats, Policies and Security Models** Peter Szczepankiewicz, SANS Instructor, Senior Security Engineer, IBM	
9:25a	Break		
	Room C/D	**Room F**	**Univ. Hall Building, Room 2008**
9:30a	**Mobile Device Security** Michael A. Davis CEO, Savid Technologies	**DIY Command & Control For Fun And *No* Profit** David Schwartzberg, CISSP Senior Security Engineer for Strategic Account, Enterprise Accounts SE Team Lead, Sophos	**SEC 464: Bad as You Can Be in 15 Minutes (SANS Lab Session)** Peter Szczepankiewicz SANS Instructor, Senior Security Engineer, IBM
10:25a	Break		
	Room C/D	**Room F**	
10:30a	**Internet Data Security Analysis and the Botnet Threat** Michael Paradise, Assistant Vice President of IP Connectivity Network Operations, AT&T	**The Mobile Hacker's Toolkit** Dave Chronister, C|EH, CISSP, MCSE, C|HFI, Founder and Managing Technology Partner, Parameter Security	
11:30a	Lunch PAC 2nd Floor	**Keynote Address: Computational Analysis of Cognitive Signatures for Mobile Security** Newton Howard, PhD, Director of the Synthetic Intelligence Lab, Resident Scientist, Massachusetts Institute of Technology Note: Please choose fish or vegetarian meal only if you selected it during registration.	
12:55p	Break		
1:00p	Afternoon Plenary Session: Room C/D	**Hiding from the Internet** Mike Bazzell, Computer Crime Detective, Federal Bureau of Investigation	
2:15p	Break		
	Room C/D	**Room F**	
2:20p	**Mobile Platforms and Cyberwarfare: Diversity is Good; Fragility is Bad; Misplacement is Ugly** Ronald P. Loui, PhD Assistant Professor of Computer Science University of Illinois Springfield	**Mini Session 1: Mobile Phone (in)Security** Darren Holtz, Special Agent, Cybercrime Investigator Federal Bureau of Investigation **Mini Session 2: FBI Cyber Jobs** Jason Shull, Administrative Specialist Federal Bureau of Investigation Kirk Staats, Special Agent, Applicant Coordinator Federal Bureau of Investigation	
3:15p	Wrap-Up and Final Prize Drawing		

UIS
UNIVERSITY of ILLINOIS SPRINGFIELD

CSSIA
Center for Systems Security and Information Assurance
CYBER DEFENSE TRAINING CENTER

INFRAGARD
SPRINGFIELD MEMBERS ALLIANCE
PARTNERSHIP FOR PROTECTION

Social Networking Safety Tips

The following tips offer guidelines in managing the information that gets out there about you via social networking and can help keep you safe:

1. **No Such Thing as Private:** The internet is like an elephant -- it never forgets. While spoken words leave little trace and are quickly forgotten, written words endure in the online environment. Whatever you post, tweet, update, share -- even if it's deleted immediately afterwards -- has the potential to be captured by someone, somewhere, without your knowledge. This is especially true of social networking sites including private messages shared between two people and postings to a private group. There is no such thing as "private" in the world of social media because anything you put up can potentially be grabbed, copied, saved on someone else's computer and mirrored on other sites -- not to mention hacked by thieves or subpoenaed by law enforcement agencies.
2. **A Little Bird Told Me:** Every time you use Twitter, the government keeps a copy of your tweets. Sounds crazy, but it's true. According to the Library of Congress blog: "Every public tweet, ever, since Twitter's inception in March 2006, will be archived digitally at the Library of Congress.... Twitter processes more than 50 million tweets every day, with the total numbering in the billions." And experts predict the information will be searched and used in ways we can't even imagine. (This gives new meaning to the phrase "A little bird told me...")
3. **X Marks the Spot:** Be cautious about using geo-location services, apps, Foursquare, or any method which shares where you're at. When it was first introduced, Facebook's "Places" feature gave tech writer Sam Diaz pause: "Guests at a party at my home could turn my home address into a public 'place' on Facebook and my only recourse is to flag my address to have it removed... If we're all at a concert...and a friend checks in with Places, he can 'tag' the people who he's with - just as if you were tagging a person in a photo." Unlike Diaz, Carrie Bugbee -- a social media strategist -- had fun using these services until a cyberstalking incident changed her mind. One evening, while dining at a restaurant she had "checked in" at using Foursquare, Bugbee was told by the hostess that there was a call for her on the restaurant's phone line. When she picked up, an anonymous man warned her about using Foursquare because she could be found by certain people; and when she tried to laugh it off, he began verbally abusing her. Stories like this may be why far fewer women use geo-location services as compared to men; many are afraid of making themselves more vulnerable to cyberstalking.
4. **Separate Work and Family:** Keep your family safe, especially if you have a high profile position or work in a field that may expose you to high-risk individuals. Some women have more than one social networking account: one for their professional/public lives and one that's restricted to personal concerns and only involves family and close friends. If this applies to you, make it clear to family/friends to post only to your personal account, not your professional page; and don't let the names of spouses, children, relatives, parents, siblings appear there to protect their privacy. Don't let yourself be tagged in events, activities or photos that may reveal personal details about your life. If they show up, delete them first and explain later to the tagger; better safe than sorry.
5. **How Old Are You Now?** If you must share your birthday, never put down the year in which you were born. Using the month and day are acceptable, but adding the year provides an opportunity for identity theft.
6. **It's Your Fault If It's Default:** Keep track of your privacy settings and check them on a regular basis or at least monthly. *Do not assume that the default setting will keep you safe.*Many social networking sites frequently update and change settings, and often the defaults tend to make public more information than you may be willing to share. If an upcoming update is advertised in advance, be proactive and investigate it before it launches; it may offer a window during which you can privately edit or remove content before it goes live. If you wait until your account automatically switches over, your information may go public before you have a chance to deal with it.
7. **It's A Family Affair:** Make it clear to family members that the best way of communicating with you is through private messaging or email -- not posting on your page. Often, relatives who are new to social media don't understand the difference between public and private conversations and how they take place online. Don't hesitate to delete something that is too personal for fear of hurting Grandma's feelings -- just make sure you message her privately to explain your actions, or better yet, call her on the phone.
8. **You Play, You Pay...in Loss of Privacy:** Online games, quizzes, and other entertainment apps are fun, but they often pull information from your page and post it without your knowledge. Make sure that you know the guidelines of any app, game or service and do not allow it unfettered access to your information. Likewise, be cautious about responding to notes shared by friends along the lines of "10 Things You Didn't Know About Me." When you answer these and post them, you're revealing personal details about yourself that may enable others to figure out your address, your workplace, the name of your pet or your mother's maiden name (often used as an online security question), or even your password. Do enough of these over time and someone who is determined to learn all about you can read the answers, cross-reference information obtained through your friends' pages, and glean a surprising amount from these seemingly casual revelations.
9. **How Do I Know You?** Never accept a friend request from someone you don't know. This may seem like a no-brainer, but even when someone appears as a mutual friend of a friend or several friends, think twice about accepting unless you can concretely identify who they are and how they're connected to you. In many professional circles involving large organizations, all an "outsider" has to do is obtain one friend on the inside and it snowballs from there, with others thinking that a total stranger with no personal connection is an unfamiliar co-worker or occasional business associate.

Source: http://womensissues.about.com/od/onlinegroupscommunities/a/10-Social-Networking-Safety-Tips-Social-Media-Women-Girls.htm