The Risks of Social Networking

IT Security Training
April 13, 2011

Harvard Townsend
Chief Information Security Officer
Kansas State University
harv@ksu.edu
Fan, Friend or Foe?
The Risks of Social Networking
It’s not a fad...
How Do We Communicate Today?

• I can write you a letter by snail mail.
• I can write you a letter by email, without any regard for capitalization and punctuation.
• I can send you a message via Xbox Live or on my Wii.
• I can call you.
  – From my office phone or mobile device.
  – From my computer running Skype.
• We can instant message (AOL, Yahoo!, Google)
• I cn txt u, LOL.
• We can video conference.
• I can be your Facebook friend.
• I can access your Myspace page.
• I can follow you on Twitter.
• I can actually visit you in person?!
“MySpace is a place for friends.”

“MySpace is Your Space.”

“MySpace keeps you connected.”
“Giving people the power to share and make the world more open and connected.”
“Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick frequent answers to one simple question:

What are you doing?”
Great Alumni event in San Fran with 70 + K-State alumni and friends – however our car was broken into and our laptops were stolen – bummer!

Day #2 in bay area – lots of visits with K-States today followed by Alumni event tonight – it is good to be out and about promoting K-State

@DePaola all business! No time for tours on this trip.

Successful on–time flights to San Francisco! We are on our way to a late lunch and our first visits!

Headed to the Bay area in California for visits with our west coast K-State alumni & friends – flying out of MIRK this am on American.
“Delicious is a Social Bookmarking service, which means you can save all your bookmarks online, share them with other people, and see what other people are bookmarking.”
Why Use Social Media?

• It’s where the students are
• Provides a sense of community
• Seen as a forum to postulate views
• Fun way to stay connected with old friends or make new friends
• Forum for communication (individual/group/mass) and collaboration
• Allows for self-expression and self-representation
• “Democratizing innovation” (users influence products)
• “Crowdsourcing” (Wikipedia the classic example)
What Are The Security Risks?

- Malware distribution
- Cyber-bullying ("trolling," emotional abuse)

November 20, 2008

First cyber-bullying trial hears how Megan Meier, 13, killed herself after online taunts

- "Shelf-life" of information (lives forever in cyberspace)

How Tweet It Is!: Library Acquires Entire Twitter Archive
April 14th, 2010 by Matt Raymond

- Privacy concerns
  - Information about you that you post
  - Information about you that others post
  - Information about you the social networking sites collect and share with others
What Are The Security Risks?

- Can result in social engineering, identity theft, financial fraud, infected computers, stalking, child abuse, sexual predation, defamation, lawsuits, mad boyfriend/girlfriend/spouse/parent, unwanted legacy, embarrassment, … job loss
Burglars used social network status updates to select victims
I'm away from home PleaseRobMe.com

By John Leyden • Get more from this author

Posted in Music and Media, 13th September 2010 12:32 GMT
Free whitepaper – The Register Guide to Enterprise Virtualization

US police reckon a band of burglars used social network status updates to select victims.

The alleged thieves carried out an estimated 50 burglaries in and around Nashua, New Hampshire, after gaining intelligence on properties that had been left vacant from status updates on social networking sites, such as Facebook.

www.theregister.co.uk/2010/09/13/social_network_burglary_gang/
Law of Unintended Consequences
Malware Distribution

- Similar to other threats that can lead to downloading/installing malware
  - Malicious ads
  - Clickjacking (aka “likejacking”)
  - Wall posts, inbox or chat messages with links from “Friends” (hijacked user account)
  - Use sex to entice people to click on a link (see “Beach Babes Video” example above)
  - “My wallet was stolen and I’m stuck in Rome. Send me cash now.”
  - Spam email pretending to be from Facebook admins
Jessica would like to be your friend on hi5!

I set up a hi5 profile and I want to add you as a friend so we can share pictures and start building our network. First see your invitation card I attached! Once you join, you will have a chance to create a profile, share pictures, and find friends.

Invitation Card.zip
Malware Distribution

• **Koobface** is grandaddy of malware targeting Facebook; continues to evolve and infect; variety of malicious acts – steals passwords, part of botnet, send message to your FB friends, redirect search engine results, install other malware

• Spread via suspicious friend or follow request, or link

• Bogus FB groups/Pages/profiles to entice you

• Suspicious/malicious application

  mashable.com/2010/05/29/facebook-hilarious-video/
Malware Distribution

“Clickjacking” example where a “Like” button had extra malicious code that posted to all her friends a link that attempted to install Koobface if clicked on.
That Important “P” Word

privacy, : \’prī-və-sē, n. “The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.”
Who’s peeking?

- Friends\family
- Friends of friends\family
- Parents
- Employers and co-workers
  - Dec 2009 study commissioned by Microsoft said 79% of recruiters & hiring mgrs researched applicants online
  - CareerBuilder.com study – 45% of employers use social networks to screen job candidates
- Customers
- Universities
- Marketing companies\vendors
- Criminals\hackers
- Government agencies (IRS, SRS!)
- EVERYONE ELSE
Linked In

Additionally, you grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to LinkedIn, including but not limited to any user generated content, ideas, concepts, techniques or data to the services, you post on LinkedIn with out any further consent, no ti ce and/or compensation to you or to any third parties. Any information you submit to us is at your own risk of loss.

Facebook

“You hereby grant Facebook an irrevocable, perpetual, non-exclusive, fully paid up and royalty-free right to publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to Facebook, including but not limited to any user generated content, ideas, concepts, techniques or data to the Facebook Service or the promotion thereof subject only to your privacy settings or (ii) enable a user to Post, including by (a) offerin a Share Link on your website and to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof.

You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license grant above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.”
A Friend of Mine Is A Friend of Yours
Choose Your Privacy Settings ▸ Customize settings

Customize who can see and comment on things you share, things on your Wall and things you're tagged in.

Preview My Profile

This is how your profile looks to most people on Facebook
Preview how your profile appears to a specific person: Start typing a friend's name

Harvard Townsend ▶ Add as Friend
Lives in Manhattan, Kansas From Manhattan, Kansas

Basic Information
Sex Male

Networks Kansas State

Harvard only shares some profile information with everyone. If you know Harvard, add him as a friend.
Choose Your Privacy Settings ▶ Customize settings

Customize who can see and comment on things you share, things on your Wall and things you're tagged in.

<table>
<thead>
<tr>
<th>Things I share</th>
<th>Posts by me</th>
<th>Family</th>
<th>Relationships</th>
<th>Interested in</th>
<th>Bio and favorite quotations</th>
<th>Website</th>
<th>Religious and political views</th>
<th>Birthday</th>
<th>Places you check in to</th>
<th>Include me in &quot;People Here Now&quot; after I check in</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default setting for posts, including status updates and photos</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Visible to friends and people checked in nearby (See an example)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[Friends Only ▼]</td>
<td>[Family ▼]</td>
<td></td>
<td></td>
<td>[Only Me ▼]</td>
</tr>
</tbody>
</table>

[Edit privacy settings](#) for existing photo albums and videos.
A Wolf in Firesheep Clothing

Firesheep is a Firefox browser add-on/plug-in that intercepts Facebook sessions (and 20+ other sites, including Twitter and Amazon) with "session hijacking".

- Allows you to become that person in FB without getting their password.
- Can post on friend's wall, send messages; can't change account settings without password.
- Freely available open source program, very easy to use on unsecured public WiFi spots.
- Also works on K-State’s wireless network!
Firesheep Defenses

• Blacksheep – another Firefox add-on: warns you if someone is running Firesheep in the area (not advisable)

• A full tunnel VPN (now available at K-State)

• Silk (WPA2) – strong encryption for wireless network (WPA2)

• Preferred: configure Facebook to encrypt all network traffic (https in the web address)
  – Change in “Account” -> ”Account Settings” -> ”Account Security”
## Account Security

Set up secure browsing (https) and login alerts.

### Secure Browsing (https)
- Browse Facebook on a secure connection (https) whenever possible

### When a new computer or mobile device logs into this account:
- Send me an email

[Save]

### Computers and mobile devices currently associated with your account:

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Time Saved</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work</td>
<td>Monday, October 25, 2010 at 8:50am</td>
<td></td>
</tr>
<tr>
<td>MacBook</td>
<td>Monday, January 10, 2011 at 3:47pm</td>
<td></td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Friday, January 7, 2011 at 6:06pm</td>
<td></td>
</tr>
<tr>
<td>Laptop @ home</td>
<td>Wednesday, October 27, 2010 at 9:28pm</td>
<td></td>
</tr>
</tbody>
</table>

### Account Activity

View your recent account activity. If you notice an unfamiliar device or location, click "end activity".

*Note: Locations and device types reflect our best guesses based on your ISP or wireless carrier.*

### Most Recent Activity

- **Location:** Unknown Location *(Approximate)*
- **Device Type:** Chrome on MacOSX

### Also Active

- **Last Accessed:** March 29 at 1:44pm
- **Device Name:** Work
- **Location:** Manhattan, KS, US *(Approximate)*
- **Device Type:** Firefox on Win7
Oh no! URL Shorteners

- bit.ly, TinyURL, ReadThisURL, NotLong
- Hides the true destination URL – no way to tell where you’re going until you click!
- Use web browser add-on offered by TinyURL and bit.ly to preview the link

http://www.hacker.com/badsite?%20infect-your-pc.html is now


DANGER! ENTER AT YOUR OWN RISK! BEWARE!
3<sup>rd</sup> Party Applications

- Games, quizzes, cutesie stuff
- Untested by Facebook – anyone can write one
- No Terms and Conditions – you either allow or you don’t
- Installation gives the developers rights to look at your profile and overrides your privacy settings!
Social Networking at Work

• Does your University have a policy? Is incidental personal use allowed? At what point does it exceed “incidental”? Discuss it with your supervisor
• Faculty and staff posting work-related information without authorization, or posting work-related information on personal pages
• K-State units should use Facebook Pages or groups rather than setting up a user profile; latter violates FB policy
• Should also be conscious of branding, making it clear whether the page is an official institutional page
• See Social Media Guidelines from K-State’s Media Relations [www.k-state.edu/media/socialmedia/](http://www.k-state.edu/media/socialmedia/)
• Possible data loss (inadvertent or malicious)
• Damage to reputation (personal or institutional)
• Regulatory compliance issues (e.g., FERPA, HIPAA)
• Personal rights issues (free speech, academic freedom)
Ethical Issues

Should you friend someone who works for you?

Should faculty accept a student’s friend request?

Should you accept your bosses’ friend request?

How much should you research job applicants?
Moral Issues

• Marriage and family therapists increasingly report that Facebook and other social media a source of marital strife; 81% of family lawyers said Facebook part of the evidence in divorce cases they handle.

• “Retrosexual” relationship – reconnecting with an old flame; FB makes it easy.

• Web site dedicated to stories of people cheating on their spouses through Facebook: www.facebookcheating.com
Moral Issues

• Warning signs:
  – Poor boundaries
  – Secrecy
  – Attraction/chemistry
  – Sharing of personal information, esp. spousal difficulties
  – Save topics of conversation for someone other than your spouse
  – Anticipate seeing “friend” more than spouse
  – Hide interaction with friend
  – Spouse does not have access to all communications with the friend
  – Spend money on friend behind spouse’s back
  – Provide special treats for the friend
  – Anticipate rituals with friend and are disappointed if they don’t happen
  – Sexual content in discussions with the friend
Tips for Safer Social Networking

1. Use a strong, unique password (don’t use the same password on multiple sites; don’t use eID password on social networking sites) and don’t share it with anyone.

2. Provide as little personal information as possible – avoid revealing birth date, address, etc.

3. Understand and customize the privacy settings in all of your social networking accounts.

4. Be careful about what you post:
   a. Photos of self or others
   b. Opinions on controversial topics
   c. Don’t rip classmates, professors, coworkers, employers, etc. – it WILL come back to haunt you.

5. Don’t post anything related to your employer (unless you’re authorized).

6. Supervise your kids’ use of social networking sites.
Tips for Safer Social Networking

7. Be suspicious of friend/follow requests, ads, 3rd party applications, chat messages, etc.

8. Minimize exploration – don’t carelessly click on lots of ads, videos, games, etc.

9. Use built-in and add-on features in web browsers to warn you of malicious sites
   a. Anti-phishing filters in IE and Firefox
   b. Web of Trust
   c. NoScript
   d. Adblock Plus
   e. Preview features of bit.ly, TinyURL

10. Trend Micro Web Reputations Services is your friend

11. Google yourself and scrutinize results

12. Think before you click!!
How To Quit Your Addiction

• How to permanently delete your Facebook account FB group (Key is to NOT use your FB account in any way for 14 days after submitting the request)

• How to deactivate your Twitter account (they claim it takes “up to 30 days to clear from our internal systems.”)

• How to delete your MySpace profile
Conclusion

• In my opinion, the value far outweighs the risk. I’d even say the dangers are exaggerated.

• Use social networking effectively and positively to establish new relationships, strengthen existing ones, innovate, learn, collaborate, and have fun.

• But beware of the risks so you can do your best to steer clear of them

• And think before you click!!
Questions?