Social Networking Security
Tobias Quosigk
ITS Information Security Office
Kennesaw State University
http://its.kennesaw.edu/infosec/
October 10, 2012
Disclaimer

- The views & opinions expressed in this presentation are my own and do not necessarily represent those of Information Technology Services, Kennesaw State University or the University System of Georgia
Overview

- Social Networking by the numbers
- Security Concerns
  - Status Updates
  - Location Services
- Photos
- Profile Information
- Applications & Add-ons
- Risk anyone?
- How to protect yourself
By the numbers

- Facebook: 1 Billion active users
- Twitter: 140+ Million active users
- LinkedIn: 175 Million users (active users not available)
- Google+: 100 Million active users
Status Updates

- To share or not to share?
  - “doesn’t like the decision my boss made today”
  - “is really looking forward to going on the cruise to the Bahamas next week!”
  - “is going to [insert bar name here] to hang out”
- Who will be able to see your status updates?
Location Services

- Add your current location to your posts (status updates, photos)
- Enabled by default for many mobile apps/platforms
- Starting to appear in desktop operating systems
- Enables strangers to track your whereabouts, monitor your habits and patterns
Photos

- Tagging photos puts names to faces
- Show your favorite places
- May expose moments you would rather like to forget, like that picture when you were drunk on Spring break
- Photo album access settings do not prevent one of your friends from leaking any of your pictures
- Great for social engineering
Profile Info / “About Me”

- Birthday
- Hometown / Where you were born
- Current location
- Schools Attended
- Favorite sports team, books, movies
- Where you work
- Your email addresses
Friends of Friends

- What is your definition of a social network “friend”?
- How about your friends’ definition?
- Which pieces of information can your friends’ friends see?
Applications & Addons

- What do they have access to?
  - Your basic info
    - Name, profile picture, gender, networks, userID, list of friends
  - Your email address(es)
  - Any other information you made public
- What does the third-party app developer do with the data they copied/harvested
What is your risk appetite?

- Have you ever forgotten your password to: your bank’s online banking site, email account, Amazon.com account
- How can you reset that password?
  - Forgotten password questions!
  - Via phone
- Identity thieves & hackers can use info from Social Networks to get into your accounts
It can’t happen to you?

- Know this guy?

- Senior Writer at Wired Magazine
The Mat Honan Story

- Amazon was called and new credit card added, later account password reset via phone
- Apple iCloud password was reset via phone
- Other accounts used iCloud account as forgotten password “secondary account”
- Gmail account was deleted
- Twitter account hacked, nasty stuff posted
- iPhone, iPad and MacBook data were remotely erased using FindMyiPhone function on iCloud.com
- This all happened in.... less than 60 minutes
The Weakest Link?

- Ask yourself:
  - How are your accounts daisy-chained together?
  - What does it take to reset any one of your online accounts?
  - Factor in the human element
How to protect yourself

- Unfriend people you don’t know/don’t talk to anymore
- Restrict access to Social Network data via Privacy settings
- Gmail: 2-step verification / 2-factor authentication
- Additional passphrases
- Choose strong password reset questions
- Use “shop safe” service to create temporary credit card numbers for use online
Questions

- Thank you for attending!
- Tobias Quosigk - tquosigk@kennesaw.edu