Security
(Computer / Network / Data)

- Not your middle school “online safety” talk
- Not theory or cutting edge research
- What you should know next year

What you should know next year

- If you are working in academia
  - Most grants require that systems be maintained and secured according to accepted best practice
  - There was one case that hit the news where a prof hired a “computer person” to do the “computer stuff”.
  - Their system was compromised and sensitive data was exposed.

  - Google “Bonnie Yankaskas UNC”

What you should know next year

- If you are working in a startup
  - It’s easy to ignore security when you are trying to get a prototype ready to attract investors.
  - You need to balance security with your other needs.
  - But it should be an informed decision.

Case Study
Twitter

http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/

- Search engines and public websites
- Gmail password recovery to expired Hotmail.com account
- (Re) Create Hotmail account, get Gmail password
- Found signup messages with cleartext password
- Set Gmail password to original password
- Use this password at Google Apps for Domains
- Uses “Secret Question” at other sites

Account Security

- Keep track of how secure each account needs to be
- Information flows from low security to high security, not from high to low
- Passwords should not be shared, or only shared between accounts that are equally secure
- “Reset” address should be a **more** secure account

Data Security

- Assume that anything you put on a free site may be compromised. You don’t control their security decisions.
- Assume that anything you put on a free site can be lost (back it up).

Security Model

- What are you protecting?
- How could it be lost / compromised?
- What is the likelihood?
- What are the risks (value)?
- What can you do to reduce the likelihood?
- What are the costs?
- What is the decision?
- Get buy in and make sure everyone knows

Resources

- seas.upenn.edu/cets/answers/linux-best-practices.html
  - Intended for the SEAS environment
  - Most of it will be useful anywhere
- sans.org/critical-security-controls/
  - Excellent list of things to be considered
  - No one does everything listed