

SAFE AND SECURE

Digital Design

Strategies for Handling Privacy Issues

Keep the Private stuff PRIVATE

- If the phone rang and someone asked you the following questions, would you answer?
 - ▣ What is your name?
 - ▣ How old are you?
 - ▣ What is your address?
 - ▣ How many people live in your home?
 - ▣ Are you male or female?
- Would you willingly give this information out online?
- Do you give it out online not knowing?

What is personal information?

- Obvious items:
 - Social Security numbers
 - Phone numbers
 - Addresses
 - Account numbers
 - Credit cards
- Not so obvious
 - School
 - Neighborhood information or descriptions
 - City or town information
 - Family information: number of children; names of family members
 - Passwords
 - pictures of self or family members
 - Physical description
 - Age
 - Birthday
 - Gender

Why can't we give out information?

- **Online predators**
 - Looking for opportunity
- **Secured and unsecured sites**
 - Computer hacking
 - Need Internet security knowledge
- **Stealing identity**
 - Identity Theft
 - Watch this video on Identify Theft
<http://www.ftc.gov/bcp/edu/microsites/idtheft/video/avoid-id-identity-theft-video.html>
 - Take Notes: definition, how identify is stolen, how to prevent it, tips to be safe, reporting, credit report effects

SOCIAL NETWORKING

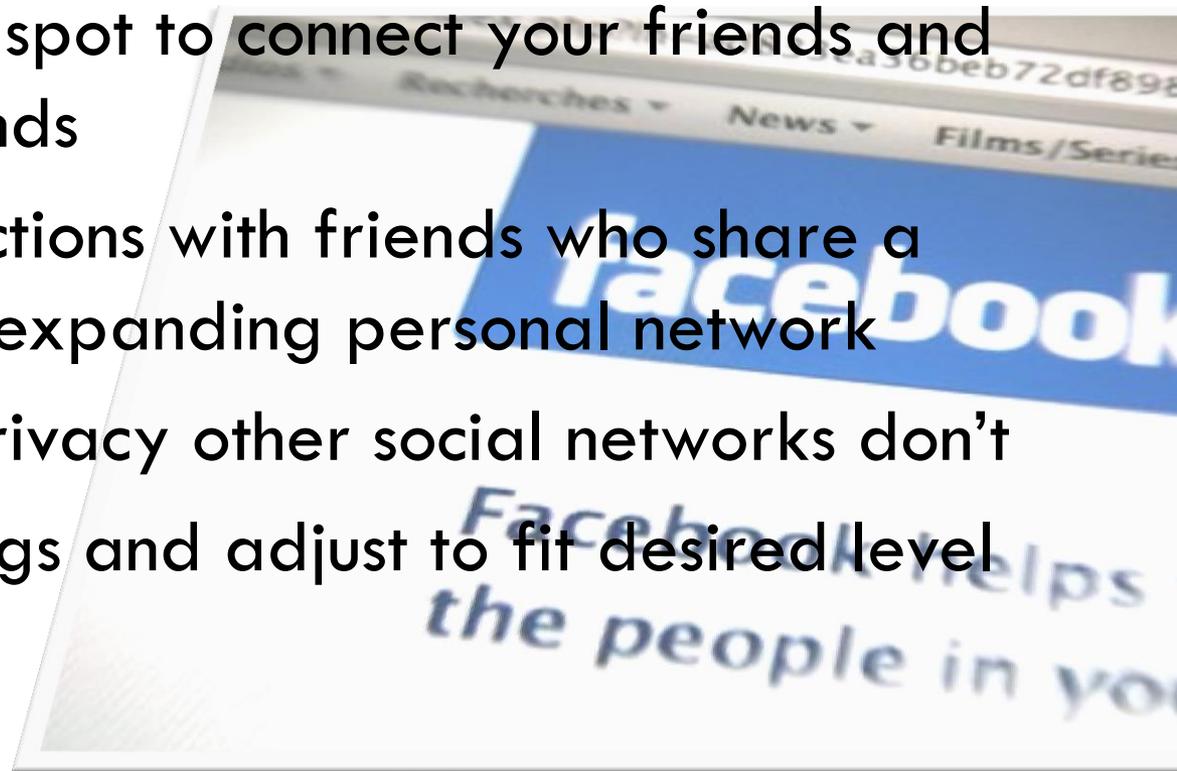
What can we find out about you?

What is social networking?

- Interaction between a group of people who share a common interest
- Virtual Communities: Facebook, MySpace
 - ▣ Social network of individuals who interact through specific media, potentially crossing geographical and political boundaries in order to pursue mutual interests or goals
- View list of Social Networking Sites from Wikipedia
http://en.wikipedia.org/wiki/List_of_social_networking_websites
Check the authenticity of each site before using

Facebook

- ❑ Social networking website
- ❑ Online gathering spot to connect your friends and your friends' friends
- ❑ Make new connections with friends who share a common interest, expanding personal network
- ❑ Offers level of privacy other social networks don't
- ❑ Set privacy settings and adjust to fit desired level of privacy



Be Safe and Secure on FACEBOOK

Profile Settings

- Most important privacy setting: who can view your profile
 - ▣ Four options for who views profile: everyone, your friends, friends of your friends or you may customize it
 - ▣ Best choice-- allow ONLY your friends to view your profile
- Second important privacy setting: Who can see your personal information
 - ▣ Includes facts about your life-- including your likes and dislikes
- Contact information-- sensitive information
 - ▣ Includes: IM Screen names, mobile phone number, home phone number, address, website and email address
 - ▣ Sensitive information—for safety reasons--should be viewable by friends only

Be Safe and Secure on FACEBOOK

Search Settings

- Search visibility
 - ▣ Find your name or not? adjust this setting accordingly
- What do you see
 - ▣ See information made visible to everyone
- Search results: outside of Facebook? on public search listings?
 - ▣ Google search...will see your Facebook page?
 - ▣ Change search setting to protect your information

Be Safe and Secure on FACEBOOK

News Feed and Wall

- What shows up in other people's news feeds about your activity
 - ▣ Do you want their home page news feed to show your comments on notes? What about photos, videos, links and relationship changes?
- What recent activity shows up on the home page.
 - ▣ Do you want people to see when you add friends or remove or change information?
- Third party Facebook ads.
 - ▣ Third party applications and ads can use your name or show your information to your friends
 - ▣ Set for no one to can access through thrid party ads or applications

Applications

- Third party applications see public search listing
 - ▣ Meaning your name, networks, profile picture and friends list
 - ▣ Change privacy settings to limit information third party applications can access

Safety Tips for Facebook users: Things to Stop Doing Now

❑ **Using a Weak Password**

- ❑ Avoid simple names or words you can find in a dictionary, even with numbers tacked on the end. Instead, mix upper- and lower-case letters, numbers, and symbols. A password should have at least eight characters. One good technique is to insert numbers or symbols in the middle of a word, such as this variant on the word “houses”: hO27usEs!

❑ **Leaving Your Full Birth Date in Your Profile**

- ❑ It’s an ideal target for identity thieves, who could use it to obtain more information about you and potentially gain access to your bank or credit card account. If you’ve already entered a birth date, go to your profile page and click on the Info tab, then on Edit Information. Under the Basic Information section, choose to show only the month and day or no birthday at all.

❑ **Overlooking Useful Privacy Controls**

- ❑ For almost everything in your Facebook profile, you can limit access to only your friends, friends of friends, or yourself. Restrict access to photos, birth date, religious views, and family information, among other things. You can give only certain people or groups access to items such as photos, or block particular people from seeing them. Consider leaving out contact info, such as phone number and address, since you probably don’t want anyone to have access to that information anyway.

❑ **Posting Your Child’s Name in a Caption**

- ❑ Don’t use a child’s name in photo tags or captions. If someone else does, delete it by clicking on Remove Tag. If your child isn’t on Facebook and someone includes his or her name in a caption, ask that person to remove the name.

❑ **Mentioning That You’ll Be Away From Home**

- ❑ That’s like putting a “no one’s home” sign on your door. Wait until you get home to tell everyone how awesome your vacation was and be vague about the date of any trip.

❑ **Letting Search Engines Find You**

My Space

- Free online community composed of personal profiles
- Aimed mostly at younger membership
- Profile typically includes: digital photo and in-depth information about personal interests
 - ▣ Amount of detail in profile determined by user
 - ▣ Submitted voluntarily
 - ▣ MySpace requires users be at least 14 years of age to join
- Members routinely send each other messages and “network” or socialize within the MySpace community
- Allows visitors to post profiles, pictures, videos and blog entries while connecting with like-minded people
- Most serious safety risk associated with using MySpace involves criminals using the site to select their next victims

MySpace Personal Internet Safety Tips

- MySpace--open forum
 - If you don't want to world to know, don't post
- If post pictures of yourself, check for inadvertently divulging personal information
 - Example: picture wearing high school shirt or local landmark
- Consider future consequences of actions
 - No naked/sexual pictures
 - Once something is posted online, it's never really erased!
- Don't assume honesty
 - Internet feels anonymous--people often lie about age, interests or general background
 - Be cautious when talking to someone meet online
- Think twice before agreeing to meet a MySpace friend in person
 - If arrange to meet--choose a public location, bring trusted friend, and make sure someone knows where you will be
- Help keep MySpace safe
 - Reporting harassment, hate speech, and other inappropriate content to the site administrators

INTERNET SECURITY



How safe is your password?

- First step in protecting online privacy creating a safe password
 - ▣ Safe Password: one a computer program or persistent individual won't easily be able to guess in a short period of time
- Password...Is it STRONG?
 - ▣ Test password.... <http://www.passwordmeter.com/>

Tips for Creating a Secure Password

- ❑ Include punctuation marks and/or numbers
- ❑ Mix capital and lowercase letters
- ❑ Include similar looking substitutions, such as the number zero for the letter 'O' or '\$' for the letter 'S'
- ❑ Create a unique acronym
- ❑ Include phonetic replacements, such as 'Luv 2 Laf' for 'Love to Laugh'

Things to avoid when creating passwords

- ❑ Don't use a password listed as an example of how to pick a good password
- ❑ Don't use a password that contains personal information (name, birth date, etc.)
- ❑ Don't use words or acronyms that can be found in a dictionary
- ❑ Don't use keyboard patterns (asdf) or sequential numbers (1234)
- ❑ Don't make your password all numbers, uppercase letters or lowercase letters
- ❑ Don't use repeating characters (aa11)

Tips for keeping your password secure

- Never tell your password to anyone
 - ▣ includes significant others, roommates, friends, etc.
- Never write your password down
- Never send your password by email
- Periodically test your current password and change it to a new one

LEGAL VS ETHICAL



Define it

- ▣ Legal – attempt to code ethical behavior; it lags behind technology; changes over time due to changes in society, reactive to society
 - Sometimes have a definitive answer
 - Determination is made by others (not you)
- ▣ Ethics – part of society, part of us, varies by person, culture, values; adapts to changes in society and technology
 - Sometimes has a definitive answer
 - You determine your course of action

The law doesn't make it "right"; being "right" doesn't make it legal