

# *Phishing Facebook*

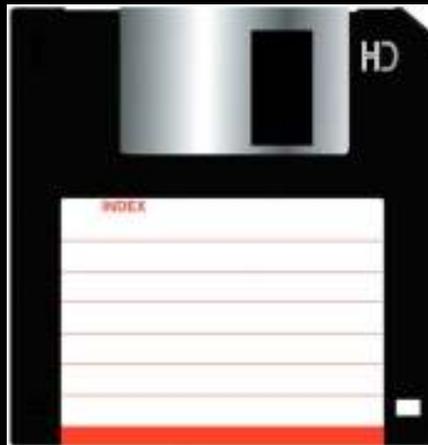
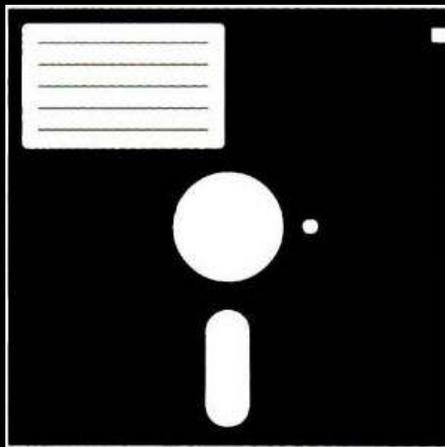
*Safety, Privacy, and Identity Theft  
on Social Networking Sites*

Gayle McCreedy  
Wayne State University



# *Who am I?*

- Academic Advisor at Wayne State
- Continuously used computers as part of my jobs since 1978



# *Technological Fluency*

Digital Immigrants

vs.

Digital Natives

- *Mark Prensky, 2001*

*When your FIRST choice  
for information  
is NOT digitized*

## *Do you ever . . .*

- Look first for information in a source other than the Internet?
- Read the manual for a new software program rather than assume that the program itself will teach you?
- Print what you need to edit rather than edit onscreen?
- Print off your emails?

# *Digital Natives*

- Freshmen in Fall 2007 were born in 1989. For them, there was never a time before:
  - **Personal computers**
  - **Microsoft and Apple**
  - **3-D Video games**
  - **The World Wide Web**
  - **Cell phones**
  - **CDs**
  - **HBO**
  - **Portable music players**
  - **PDA's**

# *Digital Natives*

- This cohort will remember these:
  - **DVDs (1995)**
  - **PayPal (1998, fully eBay in 2003)**
  - **Napster (1999)**
  - **Blogs (2000) – *as distinct from bulletin board postings and personal websites***
  - **iPods (2001)**
  - **Wireless headsets (2002)**
  - **Social networking sites (2003)**
  - **Flickr (2004)**
  - **YouTube (2005)**

# *Digital Fluency*

- The movement from Web 1.0
  - Computer/Internet as tool
  - User interacts with “it”
- To Web 2.0
  - Internet as a window to facilitate sharing and collaborating with others
  - Platform is variable
  - User interacts with “us”

# Sharing is at the Center of Web 2.0



# *Framing the Question*

- Not so much a question of *whether* students will share significant personal information online
- More a question of
  - How
  - How much
  - When
  - With whom

# *Privacy Controls*

- There is fairly high resistance to privacy controls, especially those which totally lock down the profile.
  - 1 part openness to sharing and spontaneity
  - 1 part illusion of privacy
- “Mine is just contact information, not I-can-stalk-you information”

## *Level of Engagement*

- Friendster – 2003, now 40 million users
- MyScape – 2003, now 140 million users
  - 4.6% of all internet traffic daily
- Facebook – 2004, now 21 million users, primarily college and high school students
  - 1% of all internet traffic daily
- Xanga – 2006, now 7 million users, primarily middle and high school students

# *Level of Engagement*

- In about 4 years
  - *11 users to 208 million+ users*
- Estimated 75 - 85% of college students on a social site
- Average student signs on once or twice a day
- Average use is about 20 minutes a day

# *Facebook Engagement in MI*

- Membership as of May 13<sup>th</sup>
  - Central Michigan Univ. – 25,211
  - Eastern Michigan Univ. – 18,429
  - Grand Valley State Univ. – 21,939
  - Michigan State Univ. – 60,738 (45,520)
  - Univ. of Michigan, Ann Arbor – 62,002 (4,025)
  - Wayne State Univ. – 17,677
  - Western Michigan Univ. – 27,787
    - **233,783**

# *Social Networking Sites*

- Facilitate communication between current students
- Help freshmen make connections to ease transition to college
- Provide a quick introduction to others
- Online ties can be very intense because of the quick disclosure levels

# *Social Networking Sites*

- Provides a very public forum for everyday student interactions
  - Negotiations with roommates
  - Exploring sexuality - Crushes/dating/breakups
  - Gaining experience with employers, alcohol, sometimes drugs
  - Interactions with administration, faculty, other students

# *Social Networking Site Features*

- Personal Profile
  - Age, birthday, gender, sexual orientation, address, email, work, course schedules, etc.
- Pictures, Music, Video
- Blogs
- RSS feeds
- Groups
- Twitter

# *The Illusion of Privacy*

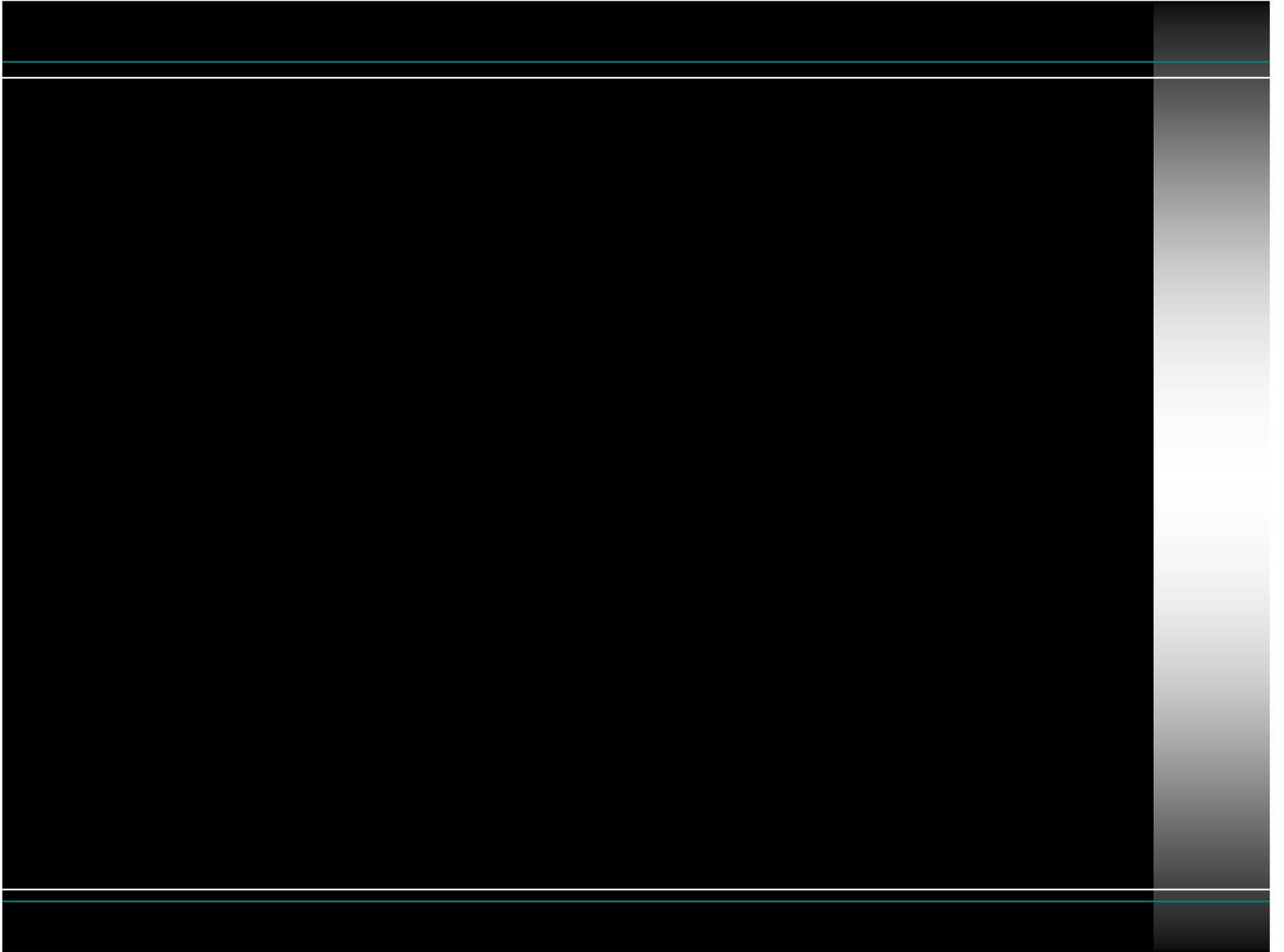
- Facebook, particularly, has carried the illusion of privacy because of its design
  - RSS feeds in fall 2006 lead to outcry
- MySpace tends to be more exhibitionistic, probably because of higher anonymity
- But both spaces can be searched from both inside and outside, with a variety of tools

# MIT Study

- A high school student doing an internship at MIT found that Facebook has an integral flaw that allows for searches within a school *without* a valid school id.
- Also, in a longer study in 2005, students at MIT were able to collect aggregate data from thousands of Facebook users across 3 schools and launch a questionnaire to ids collected from data.

# *Window of Opportunity*

- High number of users
- Constant attention and updating
- Level of personal information posted
- Illusion of privacy leads to less anonymity
  - Easy links between online persona and real student
- Systems allow for outside manipulation



## *Identity Theft – 7-10 million/year*

- Using personal information to “clone” one’s persona for the purposes of creating a second financial life
- 5% of all cases involve child SSN theft



# *Identity Theft*

- Information used
  - Full name
  - Date of birth
  - Social Security Number
  - Driver's License Number
  - Current and previous addresses
  - Current and previous employers
  - Mother's maiden name

# *Phishing*

- Con in which individual is contacted from a seemingly-reliable source to offer up personal information to “confirm” account info or reconcile a problem.
- Recent phishing attack send emails apparently from the IRS, either notifying of investigation or promising a refund.

# *Phishing for personal information*

- Phishing is typically used for financial fraud
- Pretends to be from a trusted source
- Usually pretty obvious, with experience
- Particular approach comes in waves



# *Spooofing*

- The creation of a false website to support the phishing activity, so that the site achieved by the click looks real.

# *Spear Phishing*

- Collecting information in advance of a phishing expedition in order to personalize the approach as much as possible; context-aware approach



Hey, Gayle –

I know you're busy, and I'm really sorry to bug you, but I'm kind of in a jam. Could you

[fill in blank]

## *Phishing in the wake of tragedy*

- In the wake of the VA Tech shootings, multiple scams have sprung up to phish for banking information acquired through (supposed) charitable contributions



## *Marketers use of phishing ploys*

- An advertising company in New York creates MySpace profiles for car dealerships, using a computer bot to collect contact information for persons within the geographical area. Computer-launched emails then invite the selected to become the company's "friend" with astonishing success.

## *Time to read 1984 again*

- Roelof Temmingh, security expert from South Africa, announced in April 2007 that he has developed software that will aggregate data specific to the individual across the entire web. He calls the software “Evolution.”



# *Social Networking Sites as Marketer's Dream*

Use of computer programs to collect aggregate and personalized data.

There are a variety of marketing firms who have already begun phishing for future contacts.

What is it worth to know demographic data of persons 18-25, searchable by gender, locale, tastes in music/tv/movies, and attach that data to email addresses for future contact?

*Gayle, you're such an alarmist!*

# *Privacy Issues*

- Where the disclosure of personal information on a social networking site does not lead to identity theft, but has other ramifications for the student

# *Students and the Administration*

- One of the growing ways in which student's postings on social networking sites have become problematic is the ways in which they run afoul of the college or university administration.



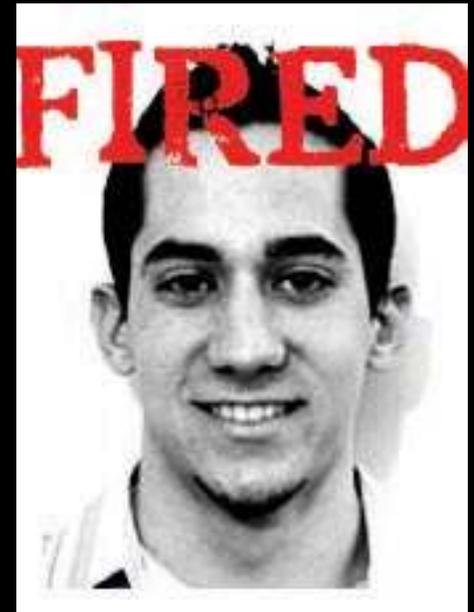
# *Students and Alcohol Policies*

- Brooke Moody of Univ. of Missouri received national attention and nearly lost her post as student assoc. president after photos of her at a party were discovered by the administration.
- Kelly Smith, a John Carroll Univ. RA was fired after pictures posted of her drinking with underage students surfaced on facebook. 4/06
- Andrew Smith-Trevino of Adelphi Univ. was fired from his job as a mentor and had to move out of the res. hall after a photo posted on facebook showed him drinking a beer (dry hall). 8/06



# *Other Student Jobs*

- Zachary Good, fired from PSU student newspaper, after postings calling a charity event self-aggrandizing. 4/07
- Two students at Algonquin College were recently fired from jobs at a local grocery chain when admitted to theft on facebook.
- Heather Armstrong was fired after writing about her employer on dooce.com, leading to term “dooced.”



# *Students-Campus Security*

- PSU campus police filed criminal trespass charges against two students and disciplined others after using facebook postings to track down fans who rushed the field after victory over Ohio. 10/05
- Princeton came under fire in 3/06 after it was revealed that they were using facebook to track down student violations.

## *Lots to find if you are looking...*

- A Western Student's profile includes interests in:
- Alternative Energy Sources, **Blunts**, Tennis, Watching Funny Movies, Lip Gloss, HOBO clutches, Black Dark Rich Coffee, Playing with My Hair, Walks through Hidden Trails, Gwen Stefani, FERGIE, Kissing, kind of.



# *Out on Facebook, Out of College*

- Jason Johnson, Univ of  
Cumberlands, expelled for being  
out on facebook, when admin  
decided that he violated code for  
“Christian life-style” 4/06
- Michael Guinn, John Brown  
Univ., expelled for posting photos  
in drag on facebook and blogging  
on Xanga that he is gay (though  
celibate). 1/06



# Student-Faculty, Syracuse

**facebook** home search global

Clearly Rachel Doesn't Know What She's Doing...EVER.'s Profile

**Description**

....and neither does Syracuses writing105 program for hiring this loser grad student who loves to pronounce her "w"s obnoxiously. Rachel, I'm sorry, but you really suck.

**Officers**

I'd rather watch my brother masturbate to midget porn with my mom than go to your class, Rachel.	<a href="#">Amanda Seideman</a>
I'd rather be eaten out by a monkey than go to your class, Rachel.	<a href="#">Colleen Smith</a>
I'd rather eat all the hair stuck in the drain of the showers than go to your class, Rachel.	<a href="#">Madison Alpern</a>
I'd rather scrape the discharge off your vagina from your yeast infection than go to your class, Rac	<a href="#">Cait Womble</a>

**Related**

- Syracu (7 peopl
- The Fir (6 peopl
- I Went (4 peopl
- I Hate

Four  
Syracuse  
students  
on  
disciplinary  
probation  
after anti-TA  
post

## *Student-Faculty*

- Univ. of Louisville students were able to get a visiting assistant professor in Psychology dismissed after emailing administration and creating a facebook site calling for her removal.

# *Student-to-Student via Sites*

Students are already aware they are being watched

- Facebook stalker
- Facecreep
- Facebush
- Facebook fuck or facewank
- MyStalker
- MySpace creeper
- Myspaceterbation

# *Stalking*

- Elvin Chaung, Hunter College, had a variety of charges filed after he coerced college women around the country into providing nude and semi-nude pictures. 6/06
  - Posed as female on social sites, lots of email and AIM contact prior to “ask.”
  - Said that she was about to fail art class because of late assignment needing nude photo, would lose scholarship if did not come up with photos.

## *Hate Speech*

- USC football players have landed in trouble with both students and administration after posting a facebook group called “white nation” which featured a photo of a Black infant in handcuffs with the caption “arrest black babies before they become criminals.”  
March 2007

# *Hate Speech*

- At WSU, there are 8 groups expressing hostility to homeless people, with more than 300 persons listed as members
  - “a few possible solutions to our little problem...also considering putting sulfuric acid into an empty liquor bottle and leaving it on the sidewalk.”
  - “those damn mother fuckers should go out and find a job and if they can't, then just go and stand in front of a bus and fuck'n kill themselves”

# *Future Employers*

- 25% of recruiting companies are surfing social networking sites to profile prospective employees
- A number of prestigious business schools have begun using site profiles to screen internship applicants
- Tech-aware companies such as Microsoft and Osram Sylvania are recruiting directly from Facebook and MySpace

# *Posts that affect interviewing*

- An applicant in a chat room posted brags about the size of his penis. This later became available to job recruiters who googled him.
- “...he rejected an applicant after searching the name of the student, a chemical engineering major, on Google. Among the things the recruiter found, she said, was this remark: ‘I like to blow things up.’”



*And don't forget . . .*

**EVERYTHING THAT WAS  
EVER POSTED  
IS SAVED ON *SOMEBODY'S*  
HARD DRIVE**

*Helping to Identify  
Risky Behaviors*

## *Start with the physical*

- NEVER CARRY A SOCIAL SECURITY CARD
- What's in your wallet – and where is it?
- How much financial information is on your laptop? Do you ever leave it unattended?
- Do you leave your laptop signed onto a social site and walk away?
- Do you store passwords on your laptop in an obvious file?

# *Use common sense*

- Turn on the Windows firewall, and don't disable the one on the university network
- Use a virus program and update it often
  - Turn on permissions to ActiveX controls
- If your computer is acting funny, or suddenly starts to slow down, assume you have a problem
- Watch the lock on the bottom of your browser window to see if the page is secure

# *Think about public sites*

- What is the level of encryption at the WiFi coffee joint you frequent?
  - Students surfing for a free wireless site may find that the security level of firewalls is so low the person at the next table can catch their logons
  - Use VPN to connect securely to your campus email
- Can people look over your shoulder and watch you type without you knowing?
- Who used the computer last? Did they leave you a “gift”?

## *Visit your profile often*

- If you've left your laptop unsecured for any length of time, your friends may have “redesigned” your profile for you.
- Watch what photos are being tagged with your name. You can't always control what pictures other people post, but you should be aware.
- If you are not using a site any longer, kill the id. You can save your blogs and pictures elsewhere.

# *Don't be a phish*

- **NEVER CLICK THE LINK**
  - Your bank is unlikely to send you an unsolicited email. If you think you really might be in trouble, go to their site and sign in to check.
- **CLOSE THE BROWSER WINDOW BETWEEN TRANSACTIONS**
  - Some programs can pick up the password you enter on the next site. Open a new window if you are handling financial data.

## *Try to disassociate your online self from your real self*

- Do not use your real name if you can help it
- Don't post your actual address – your friends already know where you live
- Don't post your cell phone number – ask any popular athlete on campus
- Don't post where you are going, just where you've been – unless you really *like* surprises

# *Remember the “rules”*

- The “poster” rule
  - When making decisions about how much personal information to post, imagine that info on a large, colorful poster on the side of a bus driving through the city.
- The “grandmother” rule
  - Are these photos ones that your grandmother could see and you wouldn’t have to get defensive?

## *And the “good parent” rule*

- If you are on social networking sites and you have a child, are you adequately protecting them?
  - Posting personal information about yourself that would allow a predator to find your child?
  - Posting pictures of your child with his/her name?
  - Blogging about your experiences as a parent with details such as school names?

## *Think about online financial transactions*

- Designate only one credit card for online purchases
- Use multiple emails, and only one of them for financial transactions
- Never use a debit card online – there is absolutely no protection for identity theft and no redress when your account is emptied

## *When it comes to jobs*

- Clean up your online persona **before** you start applying for serious jobs.
- Don't give out your social security number on any form or in an interview until you are hired. Only payroll needs to know that.
- If you are posting a résumé, ask how employers gain access. Never put your real address or date of birth on a posted résumé.

## *When your reputation reeks but you really need the job*

- Students can do their own research on their online reputations via the sites and Google
- Ask sites to remove information if possible, and have friends remove damaging photos
- If it's really bad, try a professional company like Naymz or ReputationDefenders
- Last resort, be prepared to confront the issue in an interview

## *Be vigilant about your finances*

- **Know when your bills typically arrive and be suspicious if one goes missing**
- **Check your monthly statements for odd charges for places you don't remember visiting**
- **If you received an actual credit card in the mail that you didn't request – not just an offer – you need to assume that identity theft is happening to you **now****

## *If your information gets compromised*

- Alert the bank, the credit card company, etc.
- If you believe your Social Security Number has been stolen, place a fraud alert on your credit reports. This will help stop the thief from opening new credit accounts in your name.

# *Use Common Sense*

If something seems odd,  
it is

## *Selected Resources*

- Mitrano, Tracy. “Thoughts on Facebook.” Cornell University, Office of Information Technologies, IT Policy Office, April 2006. [Http://www.cit.cornell.edu/oit/policy/memos/facebook.html](http://www.cit.cornell.edu/oit/policy/memos/facebook.html).
- “Poke Me,” UCLA Orientation manual, [http://www.icompass.ucla.edu/seminars/orientation\\_reference.pdf](http://www.icompass.ucla.edu/seminars/orientation_reference.pdf)
- BeSeKURE, University of Kansas site for information on student online security. <http://www.besecure.ku.edu/>
- The Privacy Rights Clearinghouse <http://www.privacyrights.org>
- The ID Theft Center <http://www.theidtheftcenter.org>
- On Guard Online <http://www.onguardonline.gov>

