Privacy is important. Social networks flatten out the hierarchy of what you can say.

Obscurity is NOT security.

How are people found –

Oversharing is common.

Google searches with logical operators

Ex: “Name” AND “University” OR “High School” OR “Graduation Year”

Cyber stalking is scary stuff. Cyber stalkers love location services. They can figure out your favorite restaurants if you check in often enough and when you’ll be there.

Facebook – Best Practices

-build lists (time consuming, but doesn’t have to be done all at once and worth it in the long run) (friends, acquaintances, family, professionals)

-don’t accept all friend requests (mostly about random strangers)

-set profile to “friends only”

-turn off search engine indexing (your profile can’t turn up on google searches)

-remove unused apps (delete all those weird quizzes and things you liked when you first got your facebook)

-name obfuscation? (personal preference)

-obscure your profile picture (if you’re changing you’re name to avoid being found, might as well make your profile picture less recognizable)

-unlike irrelevant pages, leave old groups (little things go a long way during hiring process)

-disable instant personalization

-disallow using your likeness in ads

-disallow third party sites from using you in ads

-set review tagged posts before allowing them to ON (this does not remove the tag from the original poster, just from your own wall)

-edit your profile, define limits of who sees what

Twitter – Best Practices

-Do not use your full name

-Use an ambiguous photo

-do not link your account to untrusted websites (news comments, untrusted apps, sites required a sign in) (trevors angry tweet got to Canada! Oh no!)

-protect your tweets

-disable location tagging (does everyone need to know where you are at every moment?)

Other sites – use your best judgment, assume everything is public

The LinkedIn Problem

By it’s nature, you want your resume-related information visible

Avoid connected to Facebook in any way

LinkedIn is a great resource, but isolate it.

Reduce your online “footprint”

Footprint is define as your online presence (number of social profiles, appearances on websites and searches, “searchability”) (Ke$ha has a bigger footprint than Austin does)

Hide these profiles from Google!

If you cannot do that…(like Facebook) CHANGE information such as names, locations, education, workplace

Delete old profiles (Are you seriously using MySpace?)

General Security Tips

-set good passwords (avoid dictionary words and personal information: your first/last name, birthday, hometown) (most common passwords: 123456, password, cats, music etc.

-good password tips: $ instead of S. random symbols. First letter of words in a movie quote

-don’t trust everything! Apps especially (basically be able to identify spam)

-never give out a password. Ever. No service will ask for your password directly

-do not connect to open Wi-Fi (like broadcasting your information on the radio) (trevor will pretend to be facebook and take your password) (don’t do your banking on BUguest) Don’t send SSN over email.

TREVOR IS WILLING TO ANSWER QUESTIONS BUT IT IS NOTED THAT HE CANNOT COMMUNICATE VIA SMOKE SIGNAL HE IS NOT FLUENT IN IT.