Security & Social Media

#oxymoron :)

---

"An oxymoron is a figure of speech in which two apparently contradictory or incompatible terms are combined to create a new idea.
assume everything is public
but organising & change need “publics” - so no choice la
1) What are you using social media for?

- Dissemination
- Mobilising support
- Information sharing
- Community building
- Discourse shaping
- Strategising

Some need more “public than others”, so make your decision on which platform to choose based on what you want it to do.

Some provide more privacy and control than others

Activity: Have an open discussion: Write down the main uses
2) Do a risk assessment

Who: Your connections
What: Potential threats
Who: Potential Asshats
What: Potential impacts
How likely: Manage your paranoia

Make a decision based on these risks, likelihood, to yourself and others.
The bigger the risk, the more careful you have to be around choosing your platform
Activity: Depending on time, can ask them to do one for something they care about. And which platform did they chose for this. Or do one in plenary
3) Get intimate with your chosen platform

- Read the fine print
- Spot data leaks
- Play with settings
- Know their politics

The more we know, the more we can try and exercise control over the spaces we choose
Know to what extent they own your data
To what extent they can share your data, with whom, with or without your permission
To what extent they can track your movements: between browsers, between sites, and consolidate this
Knowledge is powah!
- Because they can track between, important to do different strategies to anonymise yourself
- E.g. if you have 2 twitter accounts, one pseudonym, one real name, and use something like tweetdeck, can kena kantoi when accidentally post. Build walls between them to avoid leaks
- Browsers can also track, so use different ones for different social media platforms
- Use a privacy by default browser or search engines
- Do they need “real name” policies? How would it work? FB: Trans people (act on complaint, strict)
- Go through a few sites to dox themselves
  - http://checkusernames.com/
  - https://pipl.com/
- Screen caps, email forwards. Pause before you post. Is there anything that can link you? Location, topic, style of conversation etc
- Again, the more you know, the better you are able to control your privacy
- Privacy setting is your friend
- Social circle: draw out (concentric circles). Make decisions based on that. Will take a day to sort this out on FB
- First assumption: People are your data leaks. They tag you. They share you.
- How secret is a secret group?
- Any group member can add another person, and then the person can remove themselves.
- Go to transparency reports
  - https://www.google.com/transparencyreport/userdatarequests/MY/
  - https://transparency.twitter.com/country/my
  - https://govtrequests.facebook.com/country/Malaysia/2015-H2/
- Check their corporate policies
  - GNI
  - SR on FOE
- How likely will they respond to your concerns on complaints by non-state actors?
- Do they only see you if you have money sign on you? Global markets, numbers game.
- Technical community and internet activists busy building technology that is technology conscious
- Support them by getting to know them, using them, giving them feedback
- Give them some love and some pleasure in play