



Sept 1 2017

What is security culture?

A set of **behavioral norms** that a community uses to *protect members of that community*.

- It's kind of like an **etiquette** but a bit more like **solidarity**
- It's also a **methodology**
 - Extremely conditional based upon goals, circumstances
 - However there are basic principles you can follow
- It's about **prevention** of problems further down the line.
 - It's also potentially life saving.
- It is done by being mindful about how information flows.
 - Predict where and how information is most likely to “escape”.

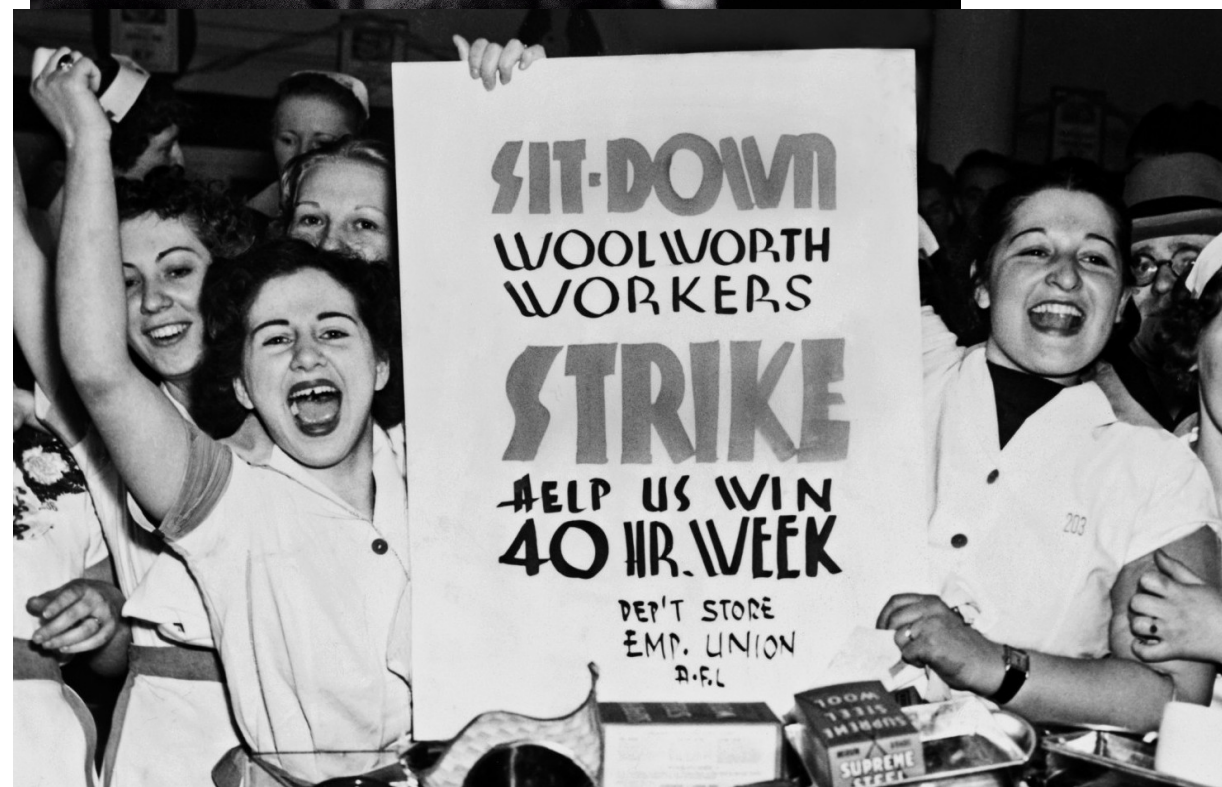
Who is security culture for?

- It's for YOU!
- It's for the people you know and love!
- Organizers no matter how (in)experienced
- People who want to protect themselves
- People who want to protect each other
- Communities who want to protect themselves
- It's for **EVERYONE!**
- Anyone can use principles of security.

Why is security culture important?

- Security: protects our freedom, well-being, rights.
- Culture: An individual can practice it, but it won't necessarily have the same advantages.
- That's why it's a security CULTURE
- Having a culture of security ensures that all members of the community are safe...
- ...especially those who need it most!
- You might not know the value of security culture until there's a problem that could have been prevented by having good security culture.
- So start now!

Scenarios & Use Cases



Scenarios & Use Cases

- **Journalist**
- **Activist/Organizer**
- **Abuse Survivor**
- **Immigrant Communities**
- **Whistleblowers**
- **Food Not Bombs**
- **Prisoner support**
- **Protests**
- **Flyering**
- **Graffiti**
- **Labor organizing**
- **Antifascist / neighborhood watch**
- **Closeted gay person**
- **Religious persecution**

What consequences do you want to avoid? (examples)

- The potential that your electronic communications could be intercepted and used against you or someone else
- Legal risks that come with the type of work you're doing
- Losing the effectiveness of your actions by e.g., losing the element of surprise
- Online bullying and threats (e.g. Gamergate)
- Physical violence by a hostile group
- Stolen identity and other garden variety cybercrime
- Facing charges, whether accidental, bogus, or otherwise
- Infiltrators or provocateurs

Security Culture, Risk, and YOU

- Security culture WORKS by treating the **disclosure of information as inherent risk**
 - The disclosure of information is managed in order to manage the potential consequences.
 - Not all information breaches result in consequences, but consequences are almost always a result of information breaches.
- Erring on the side of caution is always the right thing to do.
- Security culture CANNOT eliminate risk 100%
- Have a plan B, plan C, plan D
- Don't get in over your head!!! Take time to think it over. Don't be careless with others.
- Be accountable. Be prepared to **accept the risks and face the consequences** if your plans fail.

“If you have nothing to hide, you have nothing to worry about.”

“I have nothing to hide!”

“You're paranoid!”

“You shouldn't worry about this.”

“It'll be fiiiiiiiiiiiiiiiiine.”

... Whom does it benefit? What happened to our
5th amendment rights?



“If you have nothing to hide,
you have nothing to fear”

– Joseph Goebbels,
Reich Minister of Propaganda,
1933

- “Nothing to hide” only helps those who want to hurt you.
- **Abusers typically don't want us to be alert, practice situational awareness, or act in solidarity.**
- History repeats itself when we do not listen.
- By participating in a security culture, you are protecting the community, and the most vulnerable, even in the worst of cases.
- A community strengthened by security culture can act effectively, to defend from any threat.

How to start a security culture in your community

- Talk about it! Use it all the time! Fight ignorance! Encourage people to join you! Start clubs, host workshops! Share materials related to security culture! Remind them about Goebbels!
- Be confident! (Even if you're faking it.)
 - Learn how to gracefully redirect weird questions.
 - You're doing the right thing.
- A community practicing secure behaviors stands out less than an individual doing the same thing
- Sometimes you have to start normalizing it by being “that weirdo”:

“It's not about you, it's about your civic duty not to be a member of a predictable populace. If somebody is able to know all your preferences, habits and political views, you are causing damage to democratic society. That's why it is not enough that you are covering naughty parts of yourself with a bit of PGP, if all the rest of it is still in the nude.

Start feeling guilty. Now. It's also about your entire social environment. Your friends, your family deserves better than to end up in XKEYSCORE. You have no right to waive away their privacy. Each time you log in into Facebook or Whatsapp you are committing a felony against them.” – SecuShare developers



Don't be like this:

**SELLS SHIRT THAT SAYS : "KILL
SNITCHES"**



**TAKES TWENTY MINUTES TO BREAK SECURITY
CULTURE** memegenerator.net

SECURITY CULTURE

**MEANS I DON'T HAVE TO
BE FRIENDLY.**



quickmeme.com

Or like this:



Threat Models & Risk Assessment

- Threat models are built by doing risk assessment.
 - What is at stake, what must be protected?
 - Who is affected?
 - What steps can you take to mitigate these risks?
 - What are the ideal standards (maximum precautions)?
 - What are the minimum necessary precautions?
 - What are the opportunity costs of a precaution not taken?
 - What are the opportunity costs of taking a particular precaution?
 - Balance these opportunity costs.
 - Plan for failure. What actions will you take if plans fail?
- (In our opinion) An accurate, balanced threat model is usually best formed via calm, rational discussion between two or more individuals.

Risk assessment as applied to information security

- Social: Being aware of how information moves between people
- Tech / Electronic: Being aware of how information moves between electronic devices
- It's all about information awareness!
- Start small, take baby steps. Listen to your instincts. Err on the side of not saying anything.
 - You can plan for openness in the future
- Keeping plans simpler makes it harder for things to go wrong.

“Social” Security Quiz

- How will the information that you share travel after it leaves you?
- Is the information potentially sensitive?
- May this information become sensitive later?
- Who or what might it affect?
- Who should and should not know?
- What details should be known publicly vs privately?
- What precautions should you take?
- What are the consequences of the wrong people finding out?
- What opportunities will you miss if you don't take precautions?
- Will you require being anonymous?
- Will you require a high or low amount of visibility?
- How specific will you need to be in your communications?

001010101001111010010101Tech Security0101010100101001?!?!?!?

- How will information travel after it leaves your fingertips, or voice?
- Can you live with losing control of that information, never deleting it?
- Are you using encryption?
- Do you even need to bring a phone, laptop, or other electronic device into this? Properly done offline conversations are better than the strongest cryptography.
- Can I trust my operating system, firewall, antivirus, and network, to not leak information?
- People/companies offering you network or web services usually don't have your best interests in mind. What information are you sharing with them?
- What info can my peers on the same local network access?
- Did you research that software you're using? Is the software proprietary?
- How strong are your passwords? Don't share passwords!
- Can you delete the information? Does it still leave a residue afterwards?

001010101001111010010101Tech Security0101010100101001?!?!?!?

- Are you going to separate out your different accounts, files, devices, metadata, etc? Have them at all?
- How much personally identifiable information are you conveying through usernames, emails, online posts, profiles, etc? Will you need to use disinformation?
- How unique is your user account on the web forums that you frequent? Do you blend in? Being a stereotype helps anonymity and draws less attention.
- Did you practice and test to make sure your tech routines are working as expected? Don't wait until it's too late!
- Does your browser blend in? (Browser fingerprinting.)
- How do you determine that you are communicating with who you think you are communicating with? (MitM, impersonation, infiltration)

There are 3 main ways people mess up:

- Using technology wrong.
- Falling prey to social engineering and misplaced trust.
- Accidentally outing yourself...



▲
251
▼

Things To Do

I'm the guy in the blue shorts who got shot in the crotch last night. AMA!



submitted 1 day ago * (last edited 1 day ago) by [REDACTED]

[214 comments](#) [source](#) [share](#) [save](#) [hide](#) [give gold](#) [report](#) [hide all child comments](#)

sorted by: [top](#) ▼

you are viewing a single comment's thread.

[view the rest of the comments](#) →

▲
▼

[REDACTED] 47 points 1 day ago

Are you worried about the police pressing charges now that you've publicly identified yourself?

[permalink](#) [source](#) [embed](#) [save](#) [save-RES](#) [give gold](#) [reply](#) [hide child comments](#)

▲
▼

[REDACTED] [S]35 points 1 day ago

not really. if they wanted to arrest me I feel like they would have done so already

[permalink](#) [source](#) [embed](#) [save](#) [save-RES](#) [parent](#) [give gold](#) [reply](#) [hide child comments](#)

▲
▼

[REDACTED] 66 points 1 day ago

They might not have known who you were

[permalink](#) [source](#) [embed](#) [save](#) [save-RES](#) [parent](#) [give gold](#) [reply](#)

Man hit by gas round in viral video now faces aggravated assault on police charges

Posted: Aug 25, 2017 12:17 AM GDT

Updated: Aug 25, 2017 6:55 AM GDT

By David Baker [CONNECT](#)

By Derek Staahl [CONNECT](#)



Physical Security Quiz

- Where are the exits?
- Do you know the objects surrounding you?
- Do you know who is around you?
- What are the base normal circumstances for the time and place in question?
- Do you know what is going on around you?
- Do you have a travel route?
- Is there a chance of being followed?
- Are you able to physically defend yourself, and how?
- Will you need to have others nearby or be alone?
- Will you need to put locks on things?
- Will you need to use a camera?
- Do you have sensitive documents or devices that should be secured or shredded?
- What information do the objects around you or in photographs convey?
- What objects are more likely to turn up missing?
- Where are you exchanging information?
- How are you dressed?
- Where are the eyes, cameras, etc?
- What looks out of place?

Situational Awareness

- **Observe:** Be aware of the situation you're in.
- **Take stock:** what is out of the ordinary, and what will affect you?
 - This is the kind of thing we use everyday, e.g. at the crosswalk.
- **Adapt:** You should always be willing to change your plans and security model according to changes in situations like time, place, people, goals, contexts.
- Situational awareness aids compartmentalization (the separation of information) by helping you to identify what to separate.

How to handle paranoia

- Express your discomfort to someone who will listen, w/out winding them up.
 - Am I nuts or is ____ going on? Is ____ a credible threat? Am I being careless if I do ____? Will ____ happen?
 - Ideally the person you share your thoughts with will be grounded: will take you seriously, but won't wind you up more about it. They should be able to tell if the fear is rational. If the fear is rational, you make a plan and then don't worry. If the fear is irrational, you have no reason to worry.
 - You get to let everybody know your concerns so people are aware of what to look out for. You also clarify to yourself your concerns.
- Maybe the white van is just a white van.
- Don't be distracted by paranoia so you miss actual threats.
- A properly executed security culture can eliminate paranoia.
 - Security culture helps you plan to worry, takes the surprise out of it.
 - You must educate yourself as much as possible about the specific facts, practices, and actual/relative risks you face.

Self-care & emotional management

- Don't feed the cop in your head. Cultivate an attitude of mental freedom that will resist outside influence. Authority figures try to “break” us, we should resist domestication.
- Know your strengths and weaknesses. Practice, practice, practice.
- Taking care of yourself keeps you more functional and on top of things.
- You'll be able to protect others better when you don't overburden yourself.
- Stress has actual physical consequences.
- People are more creative when they aren't burdened by stress!
- Our strength is that we are more fluid and imaginative because we aren't constrained by the same thought patterns brought out by hierarchical modes of organization.
- Be the better you. The better you might think of better tactics and make better judgments that lead to better outcomes.
- Not taking care of yourself leads to burnout, which leads to dropout,
 - which leads to lost practical experience and lessons,
 - which leads to people reinventing the wheel,
 - and learning things the hard way over and over – as opposed to letting someone else tell you what they learned by experience.
- Good security culture teaches you what parts to actually worry about.

How to protect yourself when you are new to a community

- NOTE: We should be good to newcomers, don't make new people feel like they need to impress us!
- Be friendly, and patient, but do set boundaries even if it's scary.
- When asked for personally identifying information, don't share it. NEED to know basis. It's valid to be creeped out by such requests. Follow your intuition.
- You should almost never *have* to share your legal name, address, or place of work.
- Ask people for introductions to community members.
- Ask people for opinions about members of the community to get an idea about who is safe.
- Developing trust gradually and mindfully is key. Build real relationships based on trust, not superficiality.
- Trust your instincts and watch out for emotional manipulation.
- The first person or people you meet might not be the right people.
- Be aware that the community is sizing you up too, and your actions will definitely follow you.
- Don't accept rides or house visits unless you are sure it is safe.
- Don't drink (heavily) with strangers.

Caring for the Community

Conflicts are vulnerabilities in a community. Trying to settle some of these conflicts politely and behind closed doors before it becomes public record prevents people who want to cause us more problems from having nearly as many opportunities to disrupt our work. However, not all conflicts can be resolved privately.

In general, we recommend the following steps to handle conflicts:

- 1) Try resolving this within the community by trying to find the best personal connections between different camps and start there.
- 2) If that doesn't pan out, compile a list of things this person has done, gather signed affidavits from witnesses (name recognized by community) about actual harm witnessed, and then we present all this stuff to a group delegated to mediate the issue. The independent moderation needs to be someone with no affiliations to any party or parties involved.
- 3) Discuss the outcome among your people. If the mediation is not to your liking, then you may take it up with the court of public opinion.
- 4) Taking it up with the court of public opinion: tell them this is the findings, is this agreeable to the community? And let the public decide.

If there has been a person who presents a clear and present danger to the community, based on past behavior, and possibly future behavior, you may be morally obligated to go public with this information. Bear in mind this route is only appropriate for such company as rapists, murderers, batterers, pedophiles, cops, and advocates of genocide – NOT for getting revenge over hurt feelings or nursing a wounded ego.

Security Culture in Action

- Ask yourself: Is an unusual request? Is the person conveying a sense of urgency? Does the conversation sound scripted? Is the person trying to get information about someone?
- When someone asks a question that goes against your security guidelines, don't just stare at them awkwardly. Be clear what's not allowed.
- "That's on a need to know basis."
- "That's private/privileged information."
- "I do not wish to answer."
- "I don't know."
- "Please don't ask."
- Shake your head or use some other gesture.
- If the person has received a clear message and continues to disrespect your boundaries, this should be treated as interrogation, which is unacceptable, and you should consider their behavior disruptive and grounds for expulsion either from the group or your life.
- Security Culture is a serious matter. In certain countries and movements, people have been killed for disregarding security protocols. Those who have lived comfortably enough to not need to worry, should practice self-aware sensitivity. Cajoling those who are concerned about security is unacceptable behavior.
- If the person really needs the information, they can follow the proper channels for obtaining it, **without cheating your boundaries**.

Broadcasting and Openness

- There is value in being open. What are the things you DO want to be known?
- Even the most secretive people had their things they wanted the world to know.
- Empower people: share information that will promote safety for other people
- Distract or provide a cover for other information you want to hide
 - Politicians do this all the time
- Increase support base: Numbers may reduce the need for security tightness
 - Blending in and normalizing your political ideas can help, just try not to compromise
 - Make it easier for less committed people to get involved without stumbling upon a minefield
 - Show your pride
 - Get reputation
- Overwhelm snoopers with information until they get bored, can't sort through
- Expose enemies: “sunlight is the best disinfectant”
- There's a balance between openness and complete lockdown

Secure Organizational Structures

Security needs vary by organizational structure.

- **Less people, more discretion.**
 - The fewer people know something, the more locked down it is, but also easier to hassle.
- **More people, more openness.**
 - Hiding in the crowd helps individuals not stand out.
 - Mindful broadcasting of information, events, alerts, etc
- **More people, more discretion (security culture)**
 - Herd immunity, security culture, but hard to get full buy-in.
- **Less people, more openness.**
 - Mindful broadcasting of information, events, alerts, etc
 - Anyone providing a service to the community needs to be transparent.
 - Boston Anarchist Black Cross is an example. Also, Clearing Houses.
 - Coordinating solidarity networks.
- **Front-end security:** locked down membership
- **Back-end security:** open group, but only those who need to things, can know them
- Have a **mission statement** to define membership according to that mission.

Organizational Hierarchy

- **Hierarchies are inherently insecure.**
 - Vulnerable to infiltration
 - Single point of failure
 - Impossible burden of trust and accountability
 - Coercion and obedience
 - Brittle; not resilient enough to loss of “leaders”
- **Non-hierarchies are flexible and secure.**
 - Decentralization of resources
 - Modularity of membership base = resilient
 - Trust can be built and accounted
 - Distributed responsibility

Daft reasons why people compromise on security

- Trying to impress people
- Trying to get a date
- Trying hard to prove your credibility
- Being guilt tripped
- Intoxication
- Blinded by rage, losing temper
- Malice, personal vendettas, revenge
- Accidents, forgetfulness
- Carelessness, laziness
- Running your mouth
- Impulsiveness, urgency
- Folding in an interrogation
- Feeling the need to take a trophy, glory, that you didn't need to take
- Guy Fawkes got caught because he bragged about it in a bar
- Gossiping
- Bragging, directly or indirectly
- Desire to be accepted
- Desire for approval
- Low self esteem
- Elitism
- Trying to entertain people, funny anecdote
- Desire to establish friendships
- Retaliation for being shamed
- Not being educated on security culture

“That's a lot!” :(

- Yes, but you now have the tools to pick what to worry about and what not to worry about.
- Worry now so you don't worry later.
- Then you act accordingly and have no regret.
- Knowledge is power.
- If you've done all you can, that's good enough.
- If you have the sense to choose your risks, you will probably have the willingness to accept the consequences, positive and negative.

SCENARIOS

This is where the audience gets to pick what to talk about next.

State Surveillance

- We are in a strange period in USA's history, in which we still think we have the rights that we effectively lost because these rights have been made useless.
- The government has a large enough budget to do bulk surveillance of all electronic communications including facial recognition with driver's license
- Their budget, however large, is too limited to justify targeted surveillance on each and every individual
- They practice "signals intelligence"
- The data collected via mass surveillance can be wrong or useless
- Innocent people can be targeted for intensified surveillance based on a false positive: the best solution is encryption and Tor.
- The government uses mass surveillance, FISA, and customers consenting to give up their data to corporations, to bypass warrants
- In targeted surveillance, mail can be tampered, network can be cracked, movements and speech can be tracked, surveillance cameras or microphones can be installed, calls can be wiretapped, all without your knowledge and without serving a warrant thanks to FISA.
- Go to <https://eff.org> for more information.

State Surveillance #2

- Facial recognition evasion techniques
 - Use facial recognition camouflage like CV DAZZLE
 - Don't look straight at the camera
 - Tilt your head to the side
- Detect security cameras with night vision using phone camera
- Body temperature and body size measurers
 - You can trick the body temperature scanners to get false readings by wearing special heat reflective clothing
- Drones
- Microphones
- Police body cams
- Often times, it's not just the state that can obtain these tools of repression – ordinary citizens can do it too.

Surveillance Capitalism

- Corporations are partly to blame for the death of our privacy and erosion of civil rights.
- Tech companies have spent decades collecting and storing information about people.
- They started off by bribing individuals with free stuff, e.g. Gmail/Yahoo/MSN/etc, in exchange for information.
- They can now use social pressure to coerce individuals into giving up information, and not only that, but we pay more now than ever.
 - e.g. Individuals not on Facebook complain of being ignored by their friends and family; this 'externality' is irrelevant to corporate profits
- Corporations then sell this information to turn a profit, or surrender it to the government.

DOXXING changed everything

Snitching has never been so easy.

- Bring in your physical mail frequently as it often has your legal name.
- Maintain discipline about what information you put online, curate and cull accounts frequently.
- Use separate account for different things you do.
- Don't sign up to websites if you can help it
- Try not to use redundant usernames and passwords
- Keep your political work separate from everything else
- Be diligent about switching logins and don't be lazy about it; don't get lazy and start posting the same stuff from both
- If you want to really maintain these things as separate, change your communication style
- Does your organization really need that information?
- It's good to respect people's preferences for privacy as long as they're not messing with your privacy.
- Sometimes there is a need to meet in the middle, but trust and credibility is earned.
- If your comrade gets arrested and you don't know their name, then you can't bail them out. Or, if you are union organizing, you need to know their name and where they work in order to support them at work.
- Avoid giving personally identifiable information to people who are ill-tempered, vindictive, gossips (they may not be self-aware about it), or who you don't trust.
- Be careful about introducing people in which your trust is very situational.
- People who are ready to weaponize information you give them, are security hazards.
- Calling out behaviors on social media is almost never a good idea unless you are going public with structural issues
- Be aware that what you say about someone else on social media can affect their employment.
- You shouldn't resort to doxxing someone who is on your side unless they've done something really extreme, and you should discuss this with your group.
- Be careful of the photos you take containing metadata OR images of things (such as address) that could doxx you.
- STOP USING FACEBOOK.

Having secure conversations

Security needs vary by the type of communication method you wish to use.

- #1: Private, in-person talk, phone batteries removed
- #2: Encrypted chat
- #3: Unencrypted Phone conversation
- #4: Email or Texting or Snail mail
- Prefer voice and other complex media over plain, unencrypted text wherever possible, if you cannot use encryption, because it is harder to parse.
- Don't be led into a false sense of security. Select your words carefully, don't say dumb things, even if you use encryption!

Software to Use

- **TAILS** & Tor
- Free Software password databases like **pass**, **keypassx**, and **pwsafe**
- **LibreOffice** instead of Microsoft Word
- **Signal** (with caveats) & **Silence** (Signal fork)
- **RedPhone** and **LibrePhone** (RedPhone clone)
- **Matrix.org** instead of Discord or Riot
- **RTC** web chat with **ZRTP** encryption
- **OnionShare** to share files anonymously
- **Gobby**, **Etherpad**, and **Collabora** to build documents collaboratively
- **Goblim**, **lut.im**, **framapic.org** to upload pictures
- Metadata-erasing tools like **MAT** (available in TAILS) and **Obscuracam**
- Use Full-Disk Encryption, specifically **LUKS** (available in TAILS)
- **Bleachbit** and **wipe** tool (delete all the things)

Software to Use: Notes

- You should never use proprietary software if you can help it, since it cannot be trusted or audited.
- Signal has a backdoor: Google Play
 - Signal also blocks development forks
- Silence is fully free software
- TAILS is currently the best tool available
 - Tor Browser, preconfigured
 - Password manager: KeePassX
 - Plenty of project collaboration tools
 - You should DONATE!
- PGP + Email still gives maybe too much metadata. If you use GPG do not upload or sign your keys, use S/MIME
- Stenography (hiding in the open) is sometimes preferable to encryption
- Metadata cannot be encrypted, and it can kill you
- Don't put your data on “the cloud”, “websites”, or anyone else's server.
- **STOP USING FACEBOOK STOP USING FACEBOOK**

Email

- You can use services like **Riseup.net** and **Protonmail.com** to obtain secured email
- Self-hosting email offers data security but not anonymity unless you use a **Tor hidden service**
- **Guerrillamail** offers disposable email
- Use **PGP + MIME** (see other slide)
- Don't rely on email too much for communication
- It's still better not to use email if you can help it
- **Thunderbird** and **K-9 Mail** are the best email clients for security
- **Thunderbird + torbirdy** for email over **Tor**

Phone Numbers

- There are online databases that store people's information attached to their phone numbers.
- You should search these databases for yourself to see what you find about yourself.
- If you don't want someone knowing your legal name, for example, this might get leaked via what the databases have on your phone number.
- You should consider screening calls from unknown numbers. You can search phone numbers on the web.
- Try the Burner app, change your number frequently, buy a prepaid phone with cash only, or be careful about who you give your number to.
- Don't give your phone number to Facebook. You'll get doxx'd.

Online Databases

- In the 21st century there are online databases that store creepy amounts of identifying information about private individuals like yourselves.
- Much of it is unavoidable because our information is actually sold from company to company.
- You can prevent them from getting this information by ceasing to use social media entirely.
- If your information has been leaked to one of these databases, try to opt out or change your contact info.

Questions That Should Never Be Asked

There are certain things that are inappropriate to discuss, including:

- > your involvement or someone else's involvement with an underground group
- > someone else's desire to get involved with such a group
- > asking others if they are a member of an "underground" group
- > your participation or someone else's participation in any action that was illegal
- > someone else's advocacy for such actions
- > your plans or someone else's private plans for a future action
- > another individual's illegal acts (past, present or future)

These are always unacceptable topics regardless of whether it is rumor, speculation or personal knowledge.

Friends Don't Let Friends Use Facebook

- Whether you intend to publish information or keep a secret, Facebook is disastrous for privacy and presenting yourself as you wish to be seen.
- Facebook is philosophically against your information autonomy and believes in radical unfiltered “honesty” to everyone about everything, i.e., no boundaries
- Facebook is complex and regularly reveals new features, which has surprised users and we found it too easy to doxx ourselves.
- Facebook doesn't protect you from abusers, companies, or the government.
- Your Facebook social network graph is perfect for anyone trying to snoop on you: who-knows-who is valuable information, and has real world consequences
- Facebook demands tons of information, sells this information to third parties, and people can search for you by phone number or email address, no matter whether you've made your profile private.
- It takes skill and concerted effort to be able to fake a Facebook profile to Facebook, yet you may still get locked out.
- If something goes wrong on Facebook, there is no support team, and no phone number to call. You are the commodity, not the customer. Facebook sells YOU.

Talking to the Media

- Think about what to say before you say it and be short (20 seconds)
- Have talking points prepared, don't go off script.
- Try not to give someone an easily inflammatory sound bite if that's not your aim
- Always frame it as your opinion so you don't sound authoritative
- Don't talk unless you have your own footage.
- Pick a pseudonym and use it consistently throughout the campaign
- It helps if you are already aware of the reporter's political affiliations
- Refuse to do interviews where you don't have footage
- Come to the decision to talk as a group, not as an individual.

Affinity Groups

- An affinity group is a small group (3-12) you know and trust depending on what you're doing.
- Sometimes they even form spontaneously before they are formally recognized
- It's always better to split when you get too big
- A smaller, tight group can react quicker than a big group
- Affinity groups should be reluctant to let new people in.
- You should get to know people in your affinity group to answer the question, "How does this person react?" in a given situation.
- It can be good to have different roles, e.g. medic
- For security purposes, the group might want to have a contact person who can take care of things. Have a support person who knows the things they need to know, on a case by case basis.

Protests

- Be aware of cameras and what you're wearing. Don't be afraid to **cover your face**, regardless of whether you plan on being peaceful. Privacy is a right.
- Wear something you normally wouldn't be caught dead in.
- Be aware of police presence
- Be conscious of things you have on your person / are carrying
- Watch out for the “peace” police – marshalls are known to work with the police, not you.
- We cannot overemphasize good planning if your protesting involves anything more than simply marching, chanting, and playing music.
- Not getting arrested IS good security culture
- Don't hang around after the protest. If you want to go to a bar, go across town.
- If you want to be extra careful:
 - Don't bring your phone, or bring a properly handled burner
 - Cover your face, don't shout your friend's names
 - Don't bring anything you don't need
 - Don't bring receipts, ID, papers, etc.
 - Adopt a separate action name, or one-time use action name
 - Try not to wear anything that will make you stand out from people nearby
- When talking about it later:
 - The “passive voice” is a wonderful thing (“The window was smashed,” not “Bob smashed the window”. “Bob was maced,” not being clear by whom or why. “Mistakes were made.”)
 - Or don't talk about it at all

Camera Respectfulness

- If you are a dissident and someone takes your picture without your consent, even a coworker, I suggest you demand the immediate destruction of the image and use force if necessary. Otherwise, you may end up finding the image somewhere else, perhaps even edited in a humiliating or incriminating way.
- Don't photograph someone who is being worked on by medics.
- If you don't like having your photo taken, let people know ahead of time, to avoid awkward confrontations.
- Note that unfortunately the law is not on your side if you're trying not to be photographed in public space.

Provocateurs

- A provocateur is basically a troll, sometimes a mole, whose purpose is to endanger, exhaust, or disturb. They are intentional **dis-organizers**.
- “Always the ones suggesting using dynamite – and providing it.” Both literally and metaphorically.
- Often, these people are paid by the government to engage in risky and destructive behavior, for the purpose of destroying solidarity; but, more recently, right wingers are getting involved and it has been known that corporations will also do it for their own reasons.
- Beware of someone who comes out of nowhere and keeps inviting you to take part in their big plans.
- They usually escalate, and if you look at enough reports of this, there are classic patterns. Another way to tell a provocateur is they typically display an alarming lack of security culture.
- Government provocateurs attempt to make individuals look like more valuable arrest targets. They typically prey upon younger, less experienced people who aren't actually a threat to society and get turned into scary activist boogeymen to build someone's career and destroy their lives in the process.

Undercovers/infiltrators

- Infiltrators get into a group for the purpose of passing on information
- Their bosses want a return on their investment and the returns of nailing someone for a huge crime is more of a payoff than hassling people for small infractions
- They are motivated by a desire to get paid, promoted, and lauded as a hero
- A smart mole might learn and practice good security culture just to fit in, but it still serves as an obstacle that we want to be there
- They know things they shouldn't know and aren't smart enough to not tip people off. If someone has access to information about the group that you can't normally get, that's usually a bad sign.
- May pretend to be part of a group in order to not only snitch, but manipulate, discredit, and misdirect a group.
- They are usually eager to do thankless work, though this is not a prerequisite, and you can keep them busy. Make it so that every time they try to get information, they receive a lecture or information about security, or get redirected to do menial tasks.
- Conforming to the group's subculture is not a determinant, it's just something you notice. Just because someone doesn't know who played drums in Crass doesn't mean they aren't an anarchist. Plenty of anarchists aren't even punks. Even if they do know Crass, it doesn't prove anything.

Undercovers/infiltrators: Advice from Peter Gelderloos

- You should be using pure consensus: prevents the infiltrator from exploiting your process.
- “You probably will not know for sure if someone is a government infiltrator, and it doesn’t actually matter very much.” Because you don’t have to know.
- “...more harm has been done by accusations of infiltration than by ... bona fide infiltrators.” Infiltrators and provocateurs are more likely to accuse someone else of being an infiltrator because it is so effective at disrupting a group.
- “A key rule of security consciousness is **you don’t have to be a cop to do a cop’s work**. If someone is causing problems, regardless of whether you think she’s a cop, confront her, and if she fails to cooperate, expel her from the group. An emotionally healthy and communicative group is the best defense against infiltration.”
- “Just as political hierarchies exist to control a society, an activist organization may use hierarchy to try and control a movement. ... History shows that when governments face an enemy without a leader, whether mutinous workers or an indigenous society, they appoint one, and then negotiate, co-opt, assimilate, and control. A leaderless opposition is the hardest to defeat.”
- TL;DR: Don’t be like a paranoid Leninist sect during a purge.

Snitches

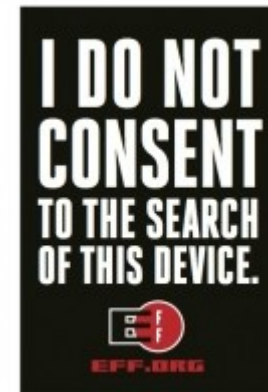
- Snitches are often people who have been involved for a fair amount of time who have different intentions than moles
 - often petty and trying to exact their revenge
 - or who have been cornered by law enforcement to the point that they break, even unrelated to their organizing
- In the past, young people who think they are going on an adventure and get busted end up snitching because they did not anticipate and accept the risks
- Snitches tend to hurt more experienced organizers with notoriety, or if law enforcement is trying to pin large charges on them
- It's not really worth law enforcement's time to try to nail someone for petty crimes, but perhaps one high profile crime (“who punched Richard Spencer?”)
- But not, e.g., Noam Chomsky because he just sits in academia
- Protect from snitches by practicing compartmentalization, so you have fewer weak links.
- “Snitches get stitches,” sometimes worse, depending on the group.
- Good relationships reduce the likelihood of snitching. Multigenerational groups, families, and close friends have strong enough trust in each other as people that snitching is unheard of, and infiltrators are easily identified.

If you BELIEVE you have FOUND a SNITCH/SPY

- They will never tell you.
- Do not try to outsmart them.
- Do investigate them.
- Have they been seen with police?
- Document your suspicions.
- Do not make open accusations without providing proof.
- Video or audiotape them
- May physically hurt you if you get in their way.
- Get away from them.
- Shut them out of the group.
- Shut the group down to foil them.
- Get a good lawyer if you believe you have said something compromising.
- You should read more about what constitutes conspiracy charges and RICO.

What to do long BEFORE being approached by cops

- Phone's lock screen should be turned on
- Turn off fingerprint recognition on iPhones
- Optional: this sticker →
- RFID blocking wallets
- Beware of stingrays
- Replicant or Cyanogenmod for your Android
- Put nailpolish on your screws so you know the device has been tampered
- Be mindful of items you don't want to be caught having
- Be aware of things that don't need to be in plain sight, keep a clean house
- Be aware that any 911 call will result in police showing up, before fire/medical
- Keep vulnerable people out of dodgy situations
- Encrypt your drives, wipe your data
- Set an app that wipes data on your device with too many brute force attempts
- Don't carry receipts and be careful about what writings and photos you have
- Be mindful that you can tie your location to places from which you purchase items



Know your rights

- Don't talk to cops. Don't answer their questions. Don't make any sudden movements.
 - If you refuse to speak to the cops, they can't write that you spoke and therefore can't make up things you said.
 - Cops don't make casual conversation with citizens. Wait to see a lawyer.
- Don't believe anything a cop promises you or says to you, period.
 - The only thing you should believe is the answer to whether you are being detained.
- When you are approached by a cop, and the cop asks you anything at all, identify yourself and then proceed with the following:
- **“AM I BEING DETAINED?”** or **“AM I FREE TO GO?”** or **“ARE WE FREE TO GO?”** if in a group. You can ask more than once.
 - If the cop answers yes, then you have to stay. If the cop answers no, then walk away.
 - If you are being detained: Breathe. Take a minute to accept the situation. Being detained can be distressing, but try to relax.
 - Be alert to what is happening around you while you are being detained.
 - If you're in a group of friends, it may be best to stick with your friends for the duration of the encounter.
 - If the cop is vague but doesn't answer firmly that you can't leave, they are trying to confuse you. Say, “Thank you officer, me and my friends are going to leave now, because you said we are free to go.” If the cop says, “No,” then stop moving immediately and stay where you are. Say, “OK officer,” and invoke your 5th amendment rights.

Know Your Rights (cont.)

- **“I WILL REMAIN SILENT AND I WANT TO SEE A LAWYER.”** You can say it in varying ways as long as you say it.
 - You have to repeat these words if you speak any other words.
 - Don’t be afraid to annoy the police officer over reinvoking your 5th amendment rights. They’re annoyed because it makes you harder to interrogate.
- If the cop starts searching you, inform the cop that you do not consent to a search.
 - Loudly say **“I DO NOT CONSENT TO THIS SEARCH.”**
 - The cop will need to obtain a warrant.
 - If you were searched without a warrant, you might be able to sue for damages. Talk to a lawyer.
 - Electronic devices with a lock screen cannot be searched for data without a warrant.
- Detained means you're not being charged (yet). You might be taken back to the station while detained.
- Arrested means you're being charged. You will be informed that you’re under arrest and will be taken back to the station.
 - Appear in court later.
 - Be aware that court records are made available online these days, with the names of the defendants and accusers.
- It does help to be familiar with the disposition of local law enforcement so you’ll know what to expect.

Security relating to arrests

- Be mindful who in your life you share the details of the arrest with
- It's your business who you talk to, unless it legally isn't
- Know that any place you're under control by police is not a safe place to speak
 - It's not unknown for cops to dress up as prisoners and get information just for the fun of it
 - Don't talk about what just happened
 - If you get a phone call, don't out yourself; saying less is better
 - This is not the time for a philosophical debate about anti-authoritarianism
 - Save it until you get out
- Supporters: Figure out where the person has been taken, where they are, what the bail is
 - Passing around a hat to get bail money for \$3000 works but not \$30,000
- The real charges you'll get will be determined at the arraignment
- This might vary by state but generally you only have to give your name and address
- Jail solidarity: when a group of people refuse to identify themselves, it can make it a nightmare for cops
 - The element of surprise is great here
 - Make sure that no one identifies anyone, inside or out
 - Make sure that people on the outside know you're doing this tactic
 - In rare cases, everyone gets released because the cops have been overwhelmed with detainees

Sexism, Racism, and Security

- Treating individuals like garbage and perpetuating systemic oppression are different risks but they should be paid attention to because they both undermine security.
- Rapists, cops, and fascist infiltrators are often racist or sexist and you can actually pick up on the warning signs if you know to look out for it.
- When we have our shit together, it's harder for them to pass as one of us.
- Some people have real lives to take care of and other folks have children to take care of. If you have serious responsibilities in your life or are marginalized such as facing the threat of deportation... You may not be able to take as many risks.
- Therefore, if your local anarchist community is less secure and not practicing good security culture, you are the vulnerable member that gets pushed out or suffers the worst punishment.
- Don't fall into a position where you have way more to lose than anyone else, and get tempted to be a snitch. Snitching is unforgivable but you should not put yourself in that position.
- It is ultimately the fault of the community when they fail to accommodate you by practicing good security. It ultimately leads to a rich white boy anarchist community.

Black bloc

- Understand and inform yourself about the risks you're taking with local laws about this tactic
- Have good plans beforehand
- Banner block!!! Think of the banner as a wall between you and the longpigs.
 - Line the outside of the bloc with banners to protect people on the edges
 - Keeping formation, and keep the banner up
 - Reinforce the banner with things like wire
- Keep it tight, keep it together, learn how to link arms, tuck your thumbs in, and don't separate (insert picture of a pair of hands doing that)
- There are lots of worthwhile things to do that aren't the high visibility, well protected areas
- Use distractions and diversions, like giant puppets or clown costumes.
- Physically cycle people being targeted from the outside to the inside
- The black bloc has a time and place, but it's not 1999 anymore
- Sometimes decentralized direct action is better than the black bloc: don't autopilot it
- Remember that prosecutors often over-prosecute
- If you have to leave at any point for some reason, at least go in pairs
- You should have at least one support person who is not there, who can take care of things
 - Inform the support person of the things they need to know, and not much more than that
- Remember that black bloc is a tool like any other tactic, and over-relying on it makes us predictable

Bad bloc



(Sorry if you're in these.)

Good bloc



Maybe paint those goggles black, and wear a darker hoodie, though.

Black Bloc Fashion tips 2017

- Wear goggles that don't cover your nose, instead of sunglasses
 - Glasses and sunglasses tend to fog up
- Cover your whole face, not just parts of it – the more covered, the safer you are
 - At least cover your nose, your eyebrows, and maybe the bags of your eyes
 - Technology is advanced; you can be identified by your nose and cover face tattoos
- If your picture has to be blurred, you're doing it wrong
- Try not to make it form fitting to avoid facial recognition technology
 - detects faces through masks tracing the contours and structure of your face
- Ideally you should cover your whole skin
- Black only - don't wear anything distinctive, but look plain, not too “black blocky”
- Pull your hoodie and mask closer – drawstrings are your friend
- Don't make it easy to pull off your mask and hoodie: double tie, drawstrings in, tie off
- Don't wear distinctive shoes! Plain black boots that aren't super heavy is good
- Get people to wear the same things, disposable is better if you can help it
- Consider wearing protective materials if you expect to get physically attacked
- Make it easy to de-bloc, wear an extra layer you can throw away if you get marked



What is comrade doing wrong?



What is comrade doing wrong?

(Answer: Adidas)



Variations on Black Bloc

Is black bloc overrated?

**It's certainly over-emphasized.
Without the element of surprise, it
doesn't work.**

**But what about giant puppets?!
That was the most important part.
BRING BACK GIANT PUPPETS!**



Anonymous Autonomous Action

- Members don't know each other
- They all take their own risks
- They show up and do an action, preferably in disguise
- They get out and never see each other again
- When they part ways:
 - they still know nothing about each other
 - they do not know where their comrades went
 - they never talk about it ever
 - even if they later talk, this design ensures that there is little information they can give about anyone else

Learn How to do Communiques

- A communique is an anonymous letter that explains an action. This is just a general introduction. Read more at <http://security.tao.ca>
- Know your printer and anyone you are trusting to work on any part of it. Don't hire a stranger.
- Buy a book of stamps with cash. Be concise, so you only need one stamp. Research the weight and thickness limits so you don't need to go to the post office and the letter is delivered.
- Don't bother cutting letters out of magazines/newspapers. Save that for art school. Check if your printer is one that contains watermarks indicating which printer the documents were printed from. Use a blue light you can purchase at <http://eff.org>. Be aware of your writing style, do not make it obviously similar. Change your punctuation marks, spelling, vocabulary, paragraph structure. Don't be obviously you.
- Pay with cash. Don't leave any fingerprints or hair on it. Don't smoke while you're working on it. Don't make or eat food. Keep pets away. Use thick enough gloves – medical gloves still transfer fingerprints. Cover your hair and roll back your sleeves or don't wear sleeves. Take your time, better late than deanonymized. Don't put your return address on it.
- Don't use more postage than necessary, don't lick the stamp, and drop it off some place you don't normally go. Not at the post office.

How to stop talking about illegal actions

- 1) It's bad to talk about or even hint at illegality, since this draws the suspicion of law enforcement and snitches.
- 2) Don't even use the word "underground," unless you're talking about hip hop.
- 3) Don't express interest in 'joining' secret groups that are known to engage in illegal activity, even if you do not intend to do anything illegal. Kick out people who do this.
- 4) If you even so much as suspect that what you're going to talk about is illegal, don't talk about it.
- 5) Gently redirect and don't reward blabbermouths.

