# Security Culture

When you're trying to change the status quo, you can expect pushback from people who benefit from the way things are, no matter how gentle or polite your methods are. Security culture is a way of keeping you and yours safe. Getting our ideas out is vital – however ideas are bulletproof, we're not. Practicing good security is altruistic: it is a part of building strong, resilient communities and caring about other people.

## DON'T

- ✖ Don't be impulsive, it only takes a moment of indiscretion to lose control of information that cannot be taken back.
- ✖ Don't draw attention to others by gossiping, bragging, or speculating. Don't let someone bait you into saying something you shouldn't.
- ✖ Don't ask questions that could draw attention or implicate others. Don't be nosy, pry, or press for useless details.
- ✖ Don't escalate conflicts needlessly or drag them into the public eye when it can be avoided.
- ✖ Don't hang onto things, either physical or digital, that could be used against you or someone else.
- ✖ Don't claim to be part of an underground organization or say that someone else is.
- ✖ Unless you're talking about spelunking or obscure music genres, don't use the phrase “the underground”, as it implies the existence of such an organization, even if there is not.
- ✖ Don't let your intoxicated and/or upset friends talk about things they normally wouldn't talk about, which they might regret later.
- ✖ Don't reward violations of security culture.
- ✖ Don't expect cars, homes, phones, emails, software, or electronics to be safe or secure means of communication.
- ✖ Don't put it on the internet, unless you have a good reason to do so. Sometimes it is necessary, and sometimes it is not. Informing the public is a valid reason, as long as you're mindful of what details you include.
- ✖ Don't let sensitive documents or electronic devices out of your sight.
- ✖ Don't talk to cops, district attorneys (DAs), prosecutors, or anyone else in law enforcement or who may be required to report. Don't talk to the press unless you know what you're doing.
- ✖ Don't let paranoia or perfectionism cause you despair. People construct bleak fantasies of things they don't understand.
- ✖ Don't get too fixed on one methodology as that can become a blind spot as situations change, which is worse than having no security at all.

## DO

- ★ Practice interrupting the urge to share. Slow down, and think about who Needs-to-Know it, and the consequences of sharing it.
- ★ Gently redirect conversations away from sensitive topics. This draws less attention to any possible exposure. Intervene if you see violations of security culture.
- ★ Become comfortable with pausing before you reply, especially you need to think about your answer. You'll end up saying better things.
- ★ If someone is being a little evasive, they probably have a good reason for it. Give people breathing room. It's OK not to know every single detail. Also: take a hint!
- ★ Avoid open conflicts with people, especially in the presence of strangers, cops, untrustworthy persons, etc. Start with a private conversation if at all possible.
- ★ You don't necessarily have to be friends with your comrades but you do need to treat each other with basic respect.
- ★ Give thought to the way that you delete or dispose of things. Burn, wipe, shred, or toss?
- ★ Educate yourself about security culture to decrease paranoia. Explain and share security culture in a way that is accessible to others. Explaining security culture is a great way to neutralize nosy or reckless people.
- ★ Compartmentalize information.
- ★ Practice situational awareness.
- ★ If you suspect a security breach, let the people affected by it know about it.
- ★ Learn basic computer security practices and encryption. Yes, some of it is difficult, but Free/Libre software hackers make activist tools that are easy and effective.
- ★ Be careful about how you float ideas of potential future actions.
- ★ Do tailor security models according to the needs of the group you're in; discuss what those needs are and set goals to meet them. Prefer done over perfection. Be willing to revise threat model as situations change.