A beginners guide to data security for activists (2025)

Issue #2, next steps

How to determine your risk level:

- What do I want to protect? Make sure you understand your assets: what data you keep and control, where it's kept, who has access to it, and what stops others from accessing it.
- Who do I want to protect it from? Who is most likely to pose a threat to you?
- How likely is it that I will need to protect it? While anything is possible in data security, consider how likely it is that a risk will actually materialize.
- How bad are the consequences if I fail? Protect assets with more sensitivity with more vigor.
- How much trouble am I willing to go through to try to prevent potential consequences? There is no such thing as perfect security. Not everyone has the same priorities, concerns, or access to resources. Understand what options you have available to you to help mitigate your unique threats. Consider your financial, technical, and social constraints.

Burner phones:

- Burner phones are meant to be used once, and then are considered "burned."
- Using a burner phone to talk to someone's everyday phone leaves a trail between you and your contact. Burners å only contact other burners.
- Never turn your burner on in proximity to your main phone.
- Identifying yourself or your contacts by name in your burner compromises your anonymity.
- Anonymous phones:
  - Anonymously buy the phone, its SIM card, and its plan. Use cash. Go to a store a bit further from your home. Walk or take other anonymous modes of transport to go buy the burner phone. Don't bring your main phone to purchase the burner.
  - Do not turn on the burner phone close to where you live, because an adversary can learn the history of a phone's physical location.
- Pseudo-anonymous phones:
  - Pseudo-anonymous phones are phones that you have purchased anonymously but you use close to where you live.

VPNs

- Virtual Private Networks (VPNs) are a way of hiding activity from your internet service provider which is regularly shared with law enforcement. VPNs disguise the flow of internet traffic entering and exiting your device, only the fact that you are using a VPN is visible. VPNs are relatively easy to install, although they do cost money.
- A VPN will not protect every aspect of anonymity.
  - Your VPN provider has access to a lot of information. While they claim not to log your information, that is a promise, not a guarantee.
  - If you don't use an HTTPS site, things like passwords, session tokens, and queries can be shared with your VPN provider and other potential adversaries in between the VPN server and your destination. HTTP is not the same level of security.

General advice:

- *Compartmentalization* is a security principle in which different identities, devices, accounts, or projects are kept separate so that they cannot be connected. This means compromising one asset should not impact the security of others. This principle can be applied to both digital and non-digital practices.
  - A *known identity* is used for things where you must declare your identity, such as paying a bill or posting on facebook.
  - An *unknown identity* could be a stable pseudonym that you regularly use. This pseudonym isn't anonymous because—if monitored for long enough—details about the owner can be put together to reveal the owner's known identity, such as the way they write, their general knowledge about topics of interest, etc. Good for online communities.
  - An *anonymous identity* should be short-term and short-lived. Create new anonymous identities regularly - consider a new one for each highly sensitive project.

General advice:

- The *need-to-know* principle means that sensitive information should be shared only when it is necessary to do so, and only to the extent necessary. This helps control the flow of information to make it more opaque to outsiders and harder to disrupt.
  - People not involved in an action should not speculate about who is involved.
  - People involved in an action should not disclose their involvement to people who are not involved.
  - People who have a specific and limited role in an action may not need to know who else is involved other than the person with whom they are communicating directly.

Phone security:

- Turn off your phone or leave it at home as much as possible, even during your day-to-day affairs and when you're not involved in any action at the time.

Phone security continued:

- Private companies track your phone at all times and this data is harvested by private companies, allowing police to access your data without a warrant. You do not need to click anything or open a link for your digital information to be traceable.
- An investigator's first step is to understand your "movement profile," and your phone's geolocation history provides a detailed picture of your daily patterns. This can also include who you call/text regularly and who you interact with on social media.
- Deviations from baseline patterns can also appear suspicious. For example, if you take your phone with you everywere, turning it off or leaving it at home is a red flag. Consider turning off your phone or leaving it at home at random intervals to obscure the baseline pattern.
- Flip phones and land lines are not encrypted.
- Don't forget to keep the physical security of the phone in mind.