OPSEC and other fun

OPSEC

We know it, we love it, we do it

1. Do not communicate outside of secure channels. Transmit only need-to-know, and only via said channels. Do not make communication public. For example, fighting about it on social media. This exposes sensitive information and people. Your political beliefs are private. If you plan to do things, do not have identifiable social media presence.
2. Need-to-know information includes potential operations, targets, timetables, and who is expected to do what. It also includes necessary resources. This is compartmentalized by each individual person involved and what role they serve. If people are not involved, they do not need to know. If you are leading an operation separately to the group, people do not need to know, except where operations may intersect.
3. Ignorance equals innocence. Do not share information that will incriminate your comrades. This includes separate operations from the group.
4. Publicly accessible information becomes sensitive when we inform people about how we are using it. Don't.
5. Planning is collaborative, and individual heroism is a risk. If you know people are planning something, swallow your ego and contribute. Communicate. In private. We win this by cooperation. Or stay silent to protect your own separate operations outside of intersection.
6. Keep things analog when possible: all digital resources should be treated as potential security risks. They have technology you don't know about that makes the tech you do know about a potential spy. Regardless of where you think it's secure.
7. Limit communication to only-necessary. This means both that you compartmentalize communication lines and that you only communicate, with only as much information as is effective, during key parts of the decided operational timeline. Or to alert other members of the group that the plan has gone awry.
8. Coded language: use it. If you need to stop an operation, a single, random, pre-decided word is more effective than a paragraph, and more secure than a communication that tells police when and where you were.
9. Assume that your devices will be accessed by police and intelligence. Assume that you will break in interrogation. Know only what you are supposed to know. Do not talk to cops except to request a lawyer. Be polite and professional. Everything about and on you will be collected as evidence. When released, you are no longer operational. Period.

10. Snitches do not get stitches: they get carefully observed and excluded from sensitive intelligence until such a time as they can be removed without exposure. A rat you know is a rat is an asset if you know how to work him, and a threat if you don't keep your mouth shut when he's around. Conversely, he will suspect he's blown if he doesn't think he's hearing some real information.
11. code words should be committed to memory instead of in any way being written down. I will also add that the military uses identifier phrases so you know whether people are in the group and if they've been compromised. The first is a call-and-response, i.e. Call "Potato", Response "Chip". We can also use secondaries and numerical codes (numbers of the day, i.e. 1, 6, an 7, which one gives as an equation, like 1+6=7). The latter is called a panic code. It's a word that is pre-selected as well and fits with the previous challenge phrase but is not the expected response, i.e. "cakes".

Revision #1
Created 2025-10-30 23:15:27 UTC by Brad
Updated 2025-10-30 23:16:54 UTC by Brad