

# Encrypted communications and threat models

Adrianna Holden-Gouveia

Website: [aholdengouveia.name](https://aholdengouveia.name)

🔗: [aholdengouveia](#)

🐦: [aholdengouveia](#)

## Accessibility Notice

This document is also available in HTML format at:

Link: <https://aholdengouveia.name/InfoSec/labs/enccomm.html>

The HTML version provides enhanced accessibility features including keyboard navigation, screen reader support, responsive design, dark mode support, and high contrast options.

## Learning Outcomes

By the end of this lab, you will be able to:

- Create a threat model for a scenario, using a structured set of questions
- Identify and prioritize risks to communications, from most to least severe
- Plan protections for each risk, including encrypted messaging, VPNs, and phone security
- Evaluate sources with the CRAAP test, and show that each one is real

## Lab Instructions

You'll put yourself in the shoes of someone in a dangerous situation, and plan how they can communicate safely. This is called threat modeling. Companies use the same steps to protect their systems.

## Pick ONE scenario

**Content note:** some of these scenarios involve violence, persecution, and people in danger. If any of them are hard for you to work on, check with me, and we'll find another option.

1. You're organizing a protest in a country that doesn't protect peaceful protest, such as Egypt or Hong Kong. You need to organize it and protect yourself and the other protesters.
2. You're visiting a country that restricts the internet. You want to communicate safely with friends and family back home, search the web, and use social media. Don't just say "use a VPN". Explain what you'd need to know about a VPN and its provider, how it works, and what protection it does and doesn't give you.
3. You're part of a minority group that the government is persecuting, such as an LGBTQ+ person in Russia, or a Uyghur Muslim in China. You want to talk to your family, and organize others to protect yourselves.
4. You're helping people escape from somewhere they're in danger, as people did on the Underground Railroad or when helping people escape Nazi Germany. You need to communicate with the next places the people you're helping will go, and plan their next steps. Modern examples include people fleeing the conflicts on the Council on Foreign Relations' Global Conflict Tracker.
5. You've found that your company's product is dangerous, and you need to tell the government while keeping yourself and your family safe. Or, you work for the government and have dangerous information the public should know, as Edward Snowden did. How do you protect yourself and your family?

If none of these appeal to you, you may come up with your own scenario, but check with me first. Background reading for each scenario is linked under Resources. Research your scenario well, so you understand what the people in it worry about.

## Build your threat model

Answer EFF's six security plan questions (linked under Resources) for your scenario, in your own words:

1. What do I want to protect?

2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?
6. Who are my allies?

Then list at least 10 risks, numbered. Focus on the technology, not the physical dangers. For example, at a protest, the risk of being pepper sprayed isn't part of this lab, but the risks of the apps and phones used to organize the protest are. Make sure you cover:

- Written communication, such as email and messaging apps
- Phone calls and text messages
- The phone itself. Almost everyone in these scenarios will have one, so explain how you'll protect it.
- Whether to use a VPN, why or why not, and what to look for in one
- Tracking, such as location sharing, app permissions, photos that include where they were taken, and hidden trackers like AirTags

As you work, think about: what's reasonable, and what's over the top? Which ways of communicating are riskier? Is there anything you're missing?

Two sample threat models, for scenarios that aren't on the list, are linked under Resources. They're laid out the way a threat model might look in industry, so they don't follow this lab's layout. Use them to see what the parts look like, but don't copy them. Your scenario is different, so your risks and plan should be too.

## Sources

You need at least 5 sources. My guide to evaluating sources, linked under Resources, shows how to do the CRAAP test, with a good and a bad example. For **each** source, include:

1. A citation, in APA or MLA style. If you want to use another style, check with me first.
2. A CRAAP test checklist or paragraph: Currency, Relevance, Authority, Accuracy, and Purpose.
3. A screenshot of the source, showing its title and date.
4. One direct quote from the source, and where it appears, such as the paragraph, section, or page.

Anything you copy word for word is a quote, so put it in quotation marks and cite it. Anything you reword, or take the ideas from, still needs a citation.

## Screenshots

Each screenshot should have your name, term, and year. One of the easiest ways to do that is make a text document with your name and term/year on your computer and save it to use all term. Any screenshots that don't include this information won't be counted.

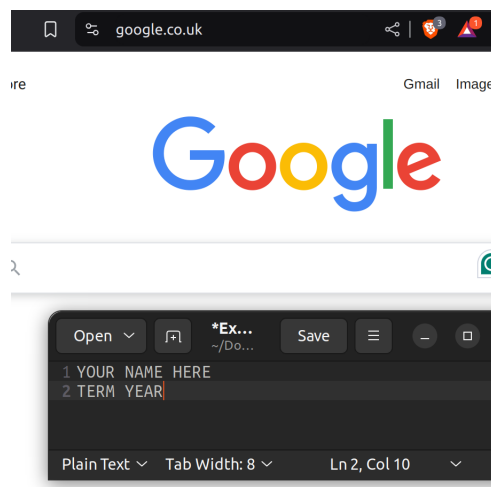


Figure 1: This is an image of what each of your screenshots should look like

## Deliverables

One file that includes:

- Which scenario you chose
- Your answers to EFF's six security plan questions
- A table of at least 10 numbered risks, ordered from most to least severe, with notes on why you ordered them that way
- A paragraph or two with your plan to reduce each risk, explaining how the plan matches the risks, and how it protects the people in your scenario as much as possible

- Your source list, with a CRAAP check, a screenshot, and a direct quote for each of your 5 or more sources

## Resources

References, a video, a PowerPoint and some notes are available at my website  
Link: <https://www.aholdengouveia.name/InfoSec/Privacy.html>

EFF Surveillance Self-Defense: Your Security Plan, with the six questions  
Link: <https://ssd.eff.org/module/your-security-plan>

Sample threat model 1: protecting a streamer's identity. Don't copy it.  
Link: <https://www.aholdengouveia.name/InfoSec/labs/threatmodel-streamer.html>

Sample threat model 2: staying safe when leaving a controlling partner. Don't copy it. **Trigger warning:** this sample talks about domestic abuse and stalking. You don't need to read it, since sample 1 shows all the same parts. Link: <https://www.aholdengouveia.name/InfoSec/labs/threatmodel-leaving.html>

EFF Surveillance Self-Defense, with guides to secure messaging, phones, and VPNs Link: <https://ssd.eff.org/>

My guide to evaluating sources Link: <https://www.aholdengouveia.name/Howtos/Sourceeval/sourceEvaluation.html>

The CRAAP test, with questions to ask about each source Link: <https://web.archive.org/web/20250814000638/https://guides.lib.uchicago.edu/c.php?g=1241077&p=9082343>

Another explanation of the CRAAP test Link: <https://libguides.butler.edu/c.php?g=117303&p=1940068>

What a threat model is Link: [https://en.wikipedia.org/wiki/Threat\\_model](https://en.wikipedia.org/wiki/Threat_model)

## Background for each scenario

Scenario 1, protests: Link: <https://www.bbc.com/news/world-middle-east-49800213>

Link: <https://www.bbc.com/news/world-asia-china-53942295>

Scenario 2, internet restrictions: Link: [https://en.wikipedia.org/wiki/Internet\\_censorship\\_and\\_surveillance\\_by\\_country](https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country)

Link: <https://cyber.harvard.edu/pubrelease/internet-control/>

Scenario 3, persecuted minorities: Link: <https://www.pbs.org/newshour/world/russias-supreme-court-effectively-outlaws-lgbtq-activism-citing-extremist-movement>

Link: <https://www.bbc.com/news/world-asia-china-22278037>

Scenario 4, helping people escape danger: Link: <https://www.nps.gov/subjects/undergroundrailroad/index.htm>

Link: <https://www.cfr.org/global-conflict-tracker>

Scenario 5, whistleblowers: Link: <https://www.bbc.com/news/technology-54013527>

Link: <https://www.whistleblowers.gov/>