

Threat Model: Staying Safe When Leaving a Controlling Partner

SAMPLE ONLY. Fictional person. Not for submission.

Trigger Warning

This sample talks about domestic abuse, stalking, and controlling relationships. You don't need to read it to do the lab. The other sample threat model, about a streamer, shows all the same parts. If this topic is hard for you, skip this one, and check with me if you'd like another option.

If any of this is happening to you, you're not alone. The National Domestic Violence Hotline is free and confidential: call 1-800-799-7233, text START to 88788, or chat at thehotline.org. Use a device the other person can't get to.

Read This First

- **This is a sample.** It shows what a threat model can look like in industry. Sam is a made-up person, and the details are invented.
- **Don't copy it.** Copied wording, risks, or controls get no credit. This scenario isn't one of the lab's choices, so you can't use it.
- **Your lab has its own requirements.** Follow the lab instructions, not this layout. Your lab needs EFF's six questions, at least 10 risks, a plan, and at least 5 sources, each with a CRAAP check, a screenshot, and a quote. This sample has no sources section like that.
- **Not professional advice.** A real safety plan should be made with a trained advocate. Some steps here, like turning off location sharing, can alert the other person, so an advocate can help you decide what to do, and when.

Accessibility Notice

This document is also available in HTML format at:

Link: <https://aholdengouveia.name/InfoSec/labs/threatmodel-leaving.html>

1 Document Control

Table 1: Document control

Field	Value
Document ID	TM-SAMPLE-02
Version	1.0
Date	October 15, 2026
System owner	Sam (fictional)
Prepared by	Adrianna Holden-Gouveia, for CIS 115
Classification	SAMPLE. Not for submission.
Next review	Weekly while Sam is moving, then every 3 months

2 Summary

Sam is leaving a controlling partner they lived with for 3 years, and is moving in with a friend. They share a phone plan, a laptop, and a car with a connected app, and the partner knows several of Sam’s passwords. The biggest risks are the partner finding Sam’s new location through their phone, a hidden tracker, or the car, and reading Sam’s messages through shared accounts. The most important protections are a new phone in Sam’s own name, securing email first, turning off location sharing, and checking for trackers, all planned with an advocate. After these protections, the remaining risk is Medium, mostly because the partner may still try to reach Sam through friends and family.

3 Scope

In scope: Sam’s phone, accounts, messages and calls, location, and the shared laptop, phone plan, and car.

Out of scope: legal protection, such as a protective order, housing, money, and physical safety plans. An advocate and a lawyer cover these.

4 Assets

Table 2: Assets to protect

Asset	Why it matters
Sam’s new address and location	If the partner finds it, Sam could be harassed or hurt
Messages and calls with family, the lawyer, and the advocate	They show Sam’s plans
Email account	It can reset the password on almost every other account
Bank and other accounts	The partner could take money or lock Sam out
Phone and phone number	The phone holds every account, and the number receives some login codes

5 Threat Actors

Table 3: Who might attack, and why

Threat actor	What they want	What they can do
The ex-partner	To find Sam, and keep control	Knows Sam’s passwords and habits, has had access to Sam’s phone, owns the phone plan
People the partner asks for help	To “help” the partner reach Sam	Ask Sam’s friends and family where Sam is

6 Assumptions

- The partner has average tech skills, and is willing to use apps and trackers that are easy to buy.
- Sam’s new phone hasn’t been touched by the partner.
- The friend Sam is staying with can be trusted.

If any of these stop being true, update this threat model, and talk to the advocate.

7 Entry Points

These are the ways the partner could reach Sam’s assets:

- Location sharing settings and family locator apps on Sam’s phone
- Any app the partner may have installed on Sam’s phone
- Sam’s bag, car, and belongings, where a tracker could be hidden
- The car’s connected app
- Accounts where the partner knows the password, or is still logged in
- The shared phone plan, laptop, and cloud accounts
- Sam’s friends, family, and social media

8 Risk Rating

Each threat gets a likelihood (how likely it is to happen) and an impact (how bad it would be), from Low to High. The overall risk comes from this table.

Table 4: How likelihood and impact combine into an overall risk

Likelihood	Low impact	Medium impact	High impact
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

9 Threat Register

Ordered from highest to lowest risk.

Table 5: Threat register

ID	Threat	Likelihood	Impact	Risk
T1	Location sharing on Sam’s phone, such as Find My, Google Maps, or a family locator app, shows where Sam is	High	High	High
T2	Stalkerware, an app that secretly reports texts, calls, and location, is on Sam’s phone	Medium	High	High
T3	A hidden tracker, such as an AirTag, is in Sam’s bag or car	Medium	High	High
T4	The car’s connected app shows where the car is parked	Medium	High	High
T5	The partner logs in to Sam’s email with a password they know, and resets Sam’s other passwords	High	High	High
T6	As owner of the phone plan, the partner sees call and text logs, or moves Sam’s number to another SIM card	High	Medium	High
T7	Shared cloud accounts sync Sam’s photos and messages to the shared laptop or a tablet, and photos can include where they were taken	Medium	Medium	Medium
T8	Friends post or tag photos of Sam, or apps with location permission show where Sam goes	Medium	Medium	Medium
T9	The shared laptop’s saved passwords and browser history show Sam’s searches for apartments, lawyers, or advocates	Medium	Medium	Medium
T10	The partner contacts Sam’s friends and family, pretending it’s an emergency, to find out where Sam is	Medium	Medium	Medium

10 Protections

Plan the timing of these with an advocate. Changing settings on the old phone or accounts can alert the partner, so some steps may need to wait until Sam is somewhere safe.

Table 6: Protections, and the threats each one reduces

ID	Protection	Threats	When
C1	Get a new phone on a new plan, in Sam’s own name, with a new number and a strong passcode. Don’t sign in to old shared accounts on it.	T1, T2, T6	Before leaving
C2	From the new phone, change the email password first, turn on two-factor authentication with an authenticator app, and sign out all other devices	T5	Before leaving
C3	Change passwords for banking, social media, and cloud accounts, and stop using shared accounts	T5, T7	After leaving
C4	Ask an advocate to help check the old phone for stalkerware, and decide when to stop using it	T1, T2	With an advocate
C5	On the new phone, keep location sharing off, and turn off location, camera, and microphone for apps that don’t need them	T1, T8	Ongoing
C6	Keep unknown tracker alerts turned on. Both iPhone and Android can warn about an unknown AirTag, and Android can also run a manual scan. Check bags and the car. If a tracker is found, talk to an advocate or the police before removing it.	T3	Ongoing
C7	Remove Sam from the car’s app, or ask the lawyer about it if the car is in the partner’s name	T4	With the lawyer
C8	Stop using the shared laptop. Use a library computer or the new phone instead.	T9	After leaving
C9	Ask friends and family not to post, tag, or share Sam’s location or new number, even if the partner says it’s an emergency	T8, T10	Before leaving

Communications

Messages and calls with family, the lawyer, and the advocate: Signal on the new phone, which is end-to-end encrypted, so only the people in the chat can read the messages. Turn on disappearing messages, and Registration Lock, which uses a Signal PIN, so no one else can sign up for Signal with Sam’s number. **Regular calls and texts:** these aren’t end-to-end encrypted, and the phone company keeps records of them, so use them only for things that aren’t sensitive.

VPN decision

A VPN isn’t a priority here. The partner isn’t watching Sam’s network. They have access to Sam’s accounts and devices. A VPN hides which websites you visit from the network you’re on, but it doesn’t stop location sharing, stalkerware, trackers, or someone who knows your password. If Sam ever has to use the old home Wi-Fi, a well-known, paid VPN would hide Sam’s browsing from that router.

11 Accepted Risk

After the protections, the remaining risk is Medium:

- The partner may still find out things through mutual friends (T10). Sam can lower this risk, but can't control what other people say.
- The partner may guess Sam's location from Sam's job or usual places. The advocate and lawyer can help with this, and it's outside this model.

12 Not Covered

This model only covers technology. Physical safety, legal protection, and housing need a safety plan made with an advocate.

13 When to Review

Review this threat model every week while Sam is moving, then every 3 months, and right away if:

- The partner seems to know something they shouldn't, such as where Sam was
- A tracker alert goes off, or an account shows a login Sam doesn't recognize
- Sam moves, changes jobs, or gets a new phone

14 References

The National Domestic Violence Hotline Link: <https://www.thehotline.org/>

National Network to End Domestic Violence: Technology Safety Link: <https://www.techsafety.org/>

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

The lab this sample goes with Link: <https://www.aholdengouveia.name/InfoSec/labs/encryption.html>