

Threat Model: Protecting a Streamer's Identity

SAMPLE ONLY. Fictional person. Not for submission.

Read This First

- **This is a sample.** It shows what a threat model can look like in industry. Riley 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.** If you have a real security problem, get help from someone who can look at your situation.

Accessibility Notice

This document is also available in HTML format at:

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

1 Document Control

Table 1: Document control

Field	Value
Document ID	TM-SAMPLE-01
Version	1.0
Date	October 15, 2026
System owner	Riley (fictional)
Prepared by	Adrianna Holden-Gouveia, for CIS 115
Classification	SAMPLE. Not for submission.
Next review	April 2027, or sooner if something under When to Review happens

2 Summary

Riley is a college student who streams video games and posts short videos, with a few thousand followers. The biggest risks are someone taking over Riley's email, and then the channel, and viewers working out Riley's real name and home address, which is called doxxing. The most important controls are a password manager, two-factor authentication with an app, separate accounts for the

channel and personal life, and checking photos and videos before posting. After these controls, the remaining risk is Low to Medium, which Riley accepts.

3 Scope

In scope: Riley’s phone and laptop, their email, streaming, and social media accounts, their messages and calls with friends, family, and sponsors, and anything Riley posts publicly.

Out of scope: the streaming platform’s own security, Riley’s school accounts, and physical safety at events. These are someone else’s responsibility, or need a separate threat model.

4 Assets

Table 2: Assets to protect

Asset	Why it matters
Real name, home address, and school	If these become public, strangers could show up in person
Personal email account	It can reset the password on almost every other account
Streaming and social media accounts	They hold Riley’s followers and income
Private messages	Friends and family share personal details there
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
Overly curious or hostile viewers	Riley’s real identity and location	Search usernames and photos, send links in chat, ask personal questions
Account takeover scammers	The channel, to resell it or run scams from it	Phishing, password reuse attacks, talking the phone company into moving Riley’s number
Fake sponsors	Riley’s login, or to install malware	Professional looking emails with “contracts” and links
Data brokers	To sell personal data	List names and addresses on people-search websites

6 Assumptions

- The streaming platform and email provider keep their own systems secure.
- No one who knows Riley in person is trying to harm them.
- Riley’s phone and laptop aren’t infected with malware today.
- Riley isn’t a target of a government or a skilled, well-funded attacker.

If any of these stop being true, update this threat model.

7 Entry Points

These are the ways an attacker could reach Riley's assets:

- Login pages for email, streaming, and social media accounts
- Riley's posts: photos, videos, the background on stream, and location tags
- Usernames shared between personal and channel accounts
- Email, direct messages, and links in chat
- The phone company's customer service, for moving a phone number
- Riley's home internet connection, through its IP address

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	Email takeover, because Riley reuses a password and has no two-factor authentication	High	High	High
T2	Photos or video reveal Riley’s home or school, through location data in the file, or a street sign, school logo, or window view in the background	Medium	High	High
T3	Location tags or location sharing, such as Snap Map, show where Riley is or goes often	Medium	High	High
T4	The same username on personal and channel accounts links the channel to Riley’s real name	High	Medium	High
T5	A fake sponsor email delivers malware, or a fake login page steals the channel password	Medium	High	High
T6	An attacker talks the phone company into moving Riley’s number to a new SIM card, and gets text message login codes	Low	High	Medium
T7	A link in chat records Riley’s IP address, which shows their city and internet provider	Medium	Medium	Medium
T8	People-search websites list the family’s address under Riley’s real name	Medium	Medium	Medium
T9	Friends tag Riley’s real name in comments or posts	Medium	Medium	Medium
T10	Phone apps have permissions they don’t need, such as location or contacts, and that data is leaked or sold	Medium	Low	Low

10 Controls

Table 6: Controls, and the threats each one reduces

ID	Control	Threats	Priority
C1	Use a password manager, with a different strong password for every account, starting with email	T1, T5	Now
C2	Turn on two-factor authentication with an authenticator app, not text messages	T1, T5, T6	Now
C3	Make a separate email address for the channel and sponsors, and a different username for personal accounts. Make personal accounts private.	T1, T4, T9	Now
C4	Before posting, check the background for signs, mail, logos, and window views. Turn off location for the camera app, and stop tagging locations.	T2, T3	Now
C5	Turn off Snap Map and other location sharing. Post about places after leaving them.	T3	Now
C6	Never open unexpected files. Check that a sponsor is real by finding the company’s website yourself, not through the email’s link.	T5	Now
C7	Add a PIN or passcode to the phone account, so the phone company won’t move the number without it	T6	This month
C8	Use a well-known, paid VPN that has had an independent audit of its no-logs promise, especially when opening links from chat or playing online games	T7	This month
C9	Ask people-search websites to remove the family’s listing, and ask friends not to tag Riley’s real name	T8, T9	This month
C10	Review app permissions every few months, and turn off what isn’t needed	T10	Ongoing

Communications

Messages with friends and family: Signal, which is end-to-end encrypted, so only the people in the chat can read the messages. **Sponsors:** the channel email only. **Phone calls and texts:** regular calls and texts aren’t end-to-end encrypted, so Riley gives sponsors a free internet phone number, such as Google Voice, and keeps their real number for people they know.

VPN decision

A VPN is worth it here, for one reason: it hides Riley’s home IP address from websites and games (T7). It doesn’t protect against stolen passwords, phishing, or a photo that shows Riley’s street, so it’s a lower priority than C1 to C6.

11 Accepted Risk

After the controls, every threat is rated Low or Medium. Riley accepts these risks:

- Someone could still guess Riley’s city from things they mention on stream, such as the weather.
- A platform data breach could leak Riley’s channel email. This is why it’s separate from their personal email.

Riley decided against Tor and a second phone. They'd be more trouble than they're worth for this threat level.

12 Not Covered

This model doesn't cover a viewer who finds Riley in person, or threats of harm. If that happens, Riley will report it to the platform and the police, and update this model.

13 When to Review

Review this threat model every 6 months, and right away if:

- The channel grows a lot, or Riley starts showing their face or real name
- An account is taken over, or Riley's address is posted online
- Riley moves, changes schools, or gets a new phone

14 References

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

EFF Surveillance Self-Defense: Protecting Yourself on Social Networks Link: <https://ssd.eff.org/module/protecting-yourself-social-networks>

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