

Bad Actors and Mindless Minions_v02

Actually it is morning for me. As a practice, I wake up every morning between 2am and 6am. This gives me sole rein of our WIFI system, and other tenants don't have to complain about my hogging the WIFI...

Weighing concerns about trust and family perception of the plans.

I'm glad to guide you through it. Before the catalog, I want to respond to what you said about your daughter.

Nothing you've described sounds like confusion to me. You've written a structured protocol with tiers, checklists, defined roles, and an honest list of open questions. You spotted that your Wi-Fi habits affect your neighbors and adjusted your schedule. Concern about AI being misused is shared by security agencies, researchers, and the companies building AI, Anthropic included. Your "armies" framing is more intense than most people's, and that's where she might push back, but holding a strong view about a real risk isn't the same as losing your grip. Of course, I only see what you write here, so she knows things I don't. If she ever raises a concern, it's worth hearing her out.

There's a practical reason to bring her into the project, too: you want these sites to outlive you.

Websites don't keep themselves going. Domains expire, hosting bills go unpaid, and passwords die with their owners unless someone else has the keys. Your daughter doesn't need to share your view of the threat to help keep your work alive. You could start with something like "I'm building a nonprofit library and I need a backup person." Succession planning deserves its own session later.

Now, here's the catalog structure. Each downloaded item gets one record with these fields:

Field	What goes in it
Item ID	A simple running number (0001, 0002...)
Title	The document's actual title
Source organization	EFF, CISA, NIST, etc.
Original URL	Where you got it, so you can check for updates
Date downloaded	The night you pulled it
Source's last-reviewed date	Printed on many guides; blank if none
Format	PDF, web page, video, software, etc.
Audience	Member, Teacher, or Nonprofit
Threat category	One of the categories below
License	e.g., Creative Commons BY, public domain, "free to read only"
Status	Downloaded → Checked → In vault
Notes	Anything worth remembering about it

Threat categories: Scams & phishing · Passwords & account takeover · Malware · Deepfakes & voice cloning · Privacy & data exposure · AI-specific risks · Incident response · General foundations, for basics that cover everything.

The Status field ties the library to your protocol. Nothing gets marked "In vault" until it's been checked on the outside workstation and carried in by hand. Over time, the dates will show you what's gone stale and needs refreshing.

My suggestion for the first night is modest: pick one source, such as EFF's Surveillance Self-Defense, download its guides, and log each one. That will reveal which fields are useful in practice, and we can adjust before the library grows large.

I can build this as a ready-to-use spreadsheet with dropdown lists for Audience, Category, and Status. Would you like that, or would you rather set it up in a database yourself, given your background?

Just for the record, I changed my radical first statement: I would like to start thinking about accumulating as much free information we can. I need to start setting up some workstations to start downloading and categorizing all the free stuff that can help us effectively build a defense against Rogue AI bots. My personal opinion is that there are bad actors with thousands of mindless minions being trained to steal identities and money from unsuspecting people. And I want to have a hands on knowledge and full toolbox to be able to thwart as many threats as possible

Checking the revised statement against known scam evidence.

Noted, and the revised version is well put. It's also closer to what's actually documented: large organized fraud operations, some staffed by thousands of workers, are increasingly using AI to write convincing messages, clone voices, and run automated bots that work around the clock. Identity theft and financial fraud are the main goals. Your "mindless minions" image fits both the bots and the people forced to run scripts in some of these operations.

This framing also works better for your audience. It names a concrete enemy, scammers after identities and money, which points directly to concrete defenses: recognize the trick, protect the accounts, know what to do if something goes wrong. That's exactly what the library is for. It might be worth putting a version of this sentence on the SneakerNetUSA site as the reason the library exists.

The plan stays the same: outside workstations, overnight downloads, everything logged in the catalog, and vetted copies carried into the vault. Whenever you're ready, I can build the spreadsheet with the dropdowns, or you can set it up in a database yourself.

