That's not my Repo and other scary children's tales

Steve Poole

Independent

Software Supply Chain Security Expert

DevOps Practice Lead

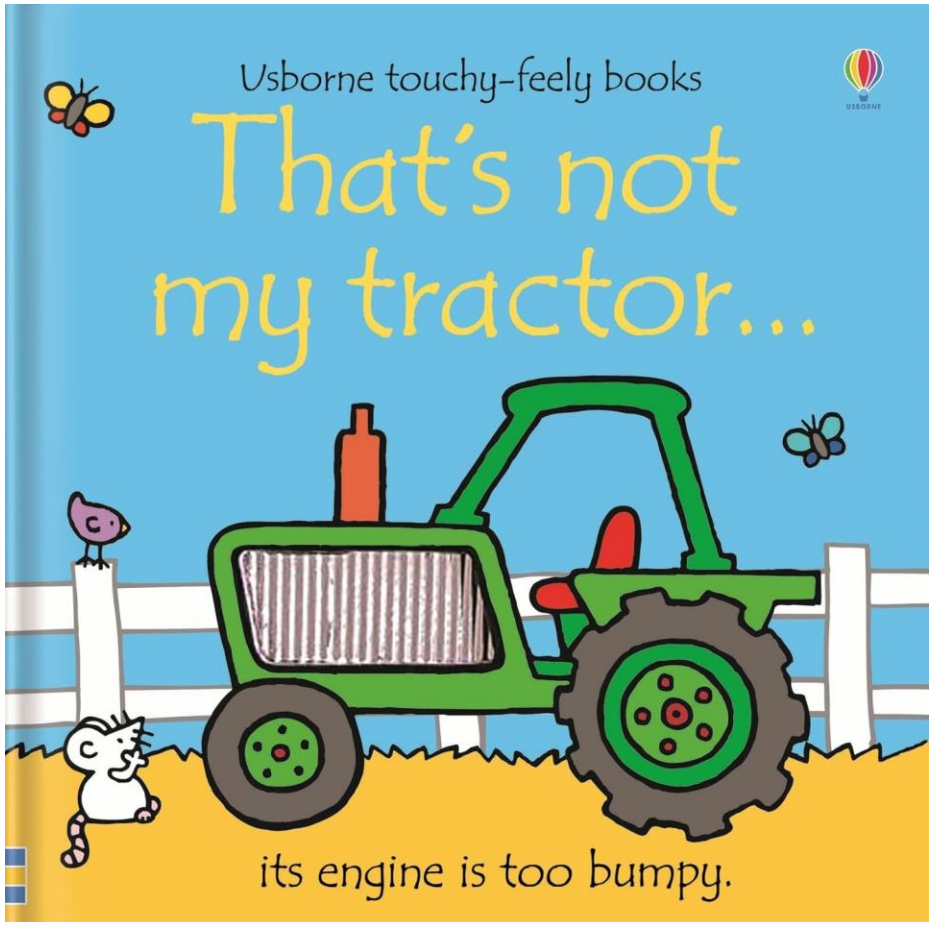
Find me on LinkedIn for further discussions or consultancy

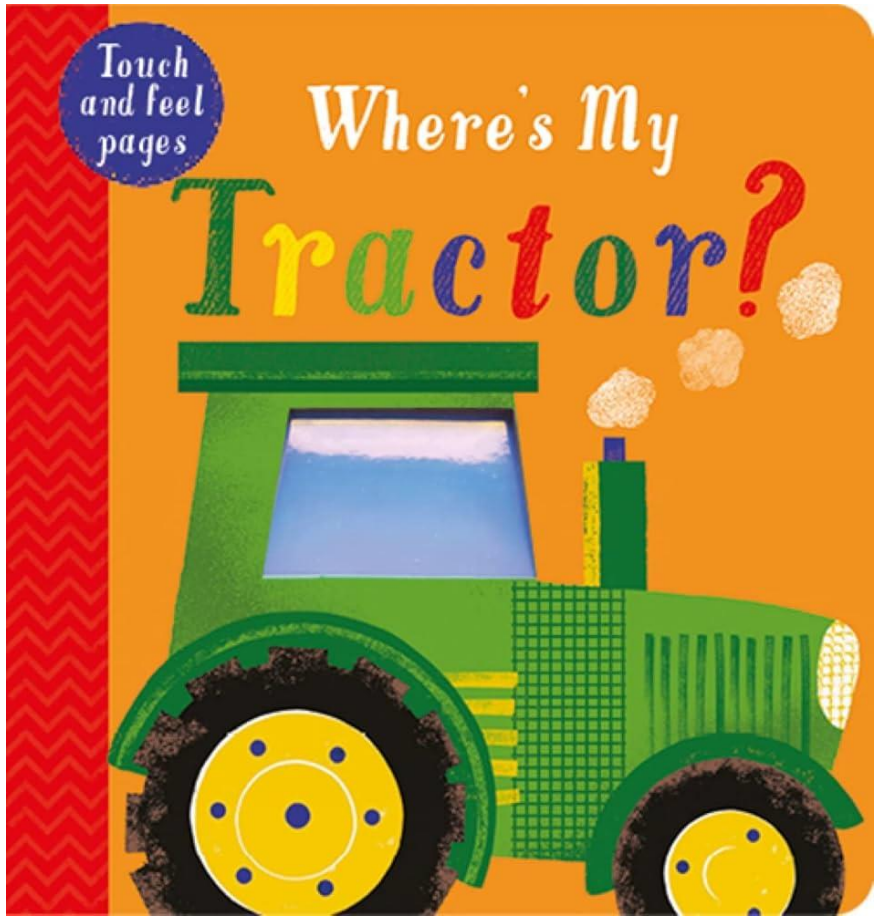
www.linkedin.com/in/noregressions/

Visit the podcast

10xinsights.dev/

This talk is inspired by

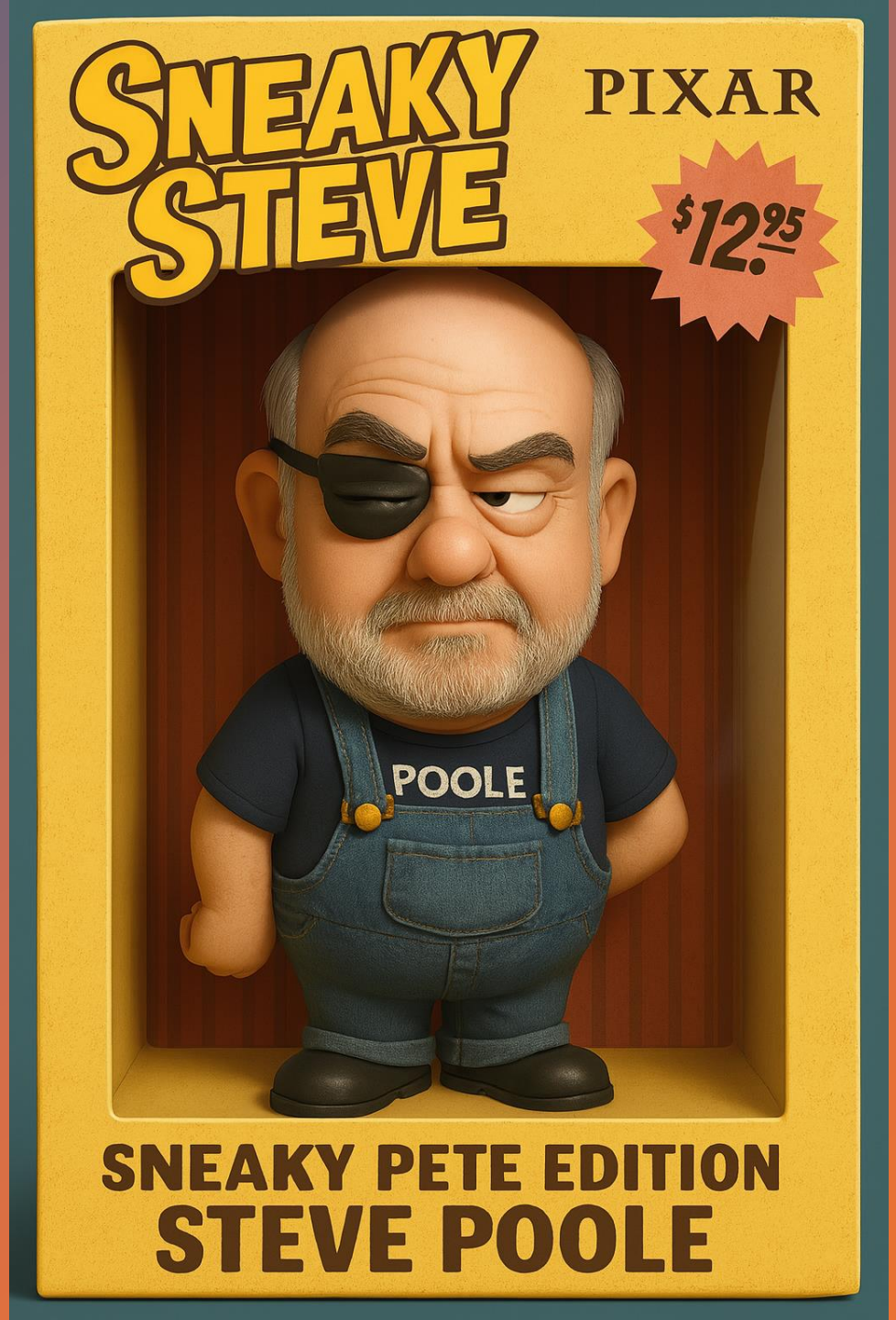




My epiphany ? that we need to talk developers about security their way, in the language, from their POV

This deck contains AI generated images

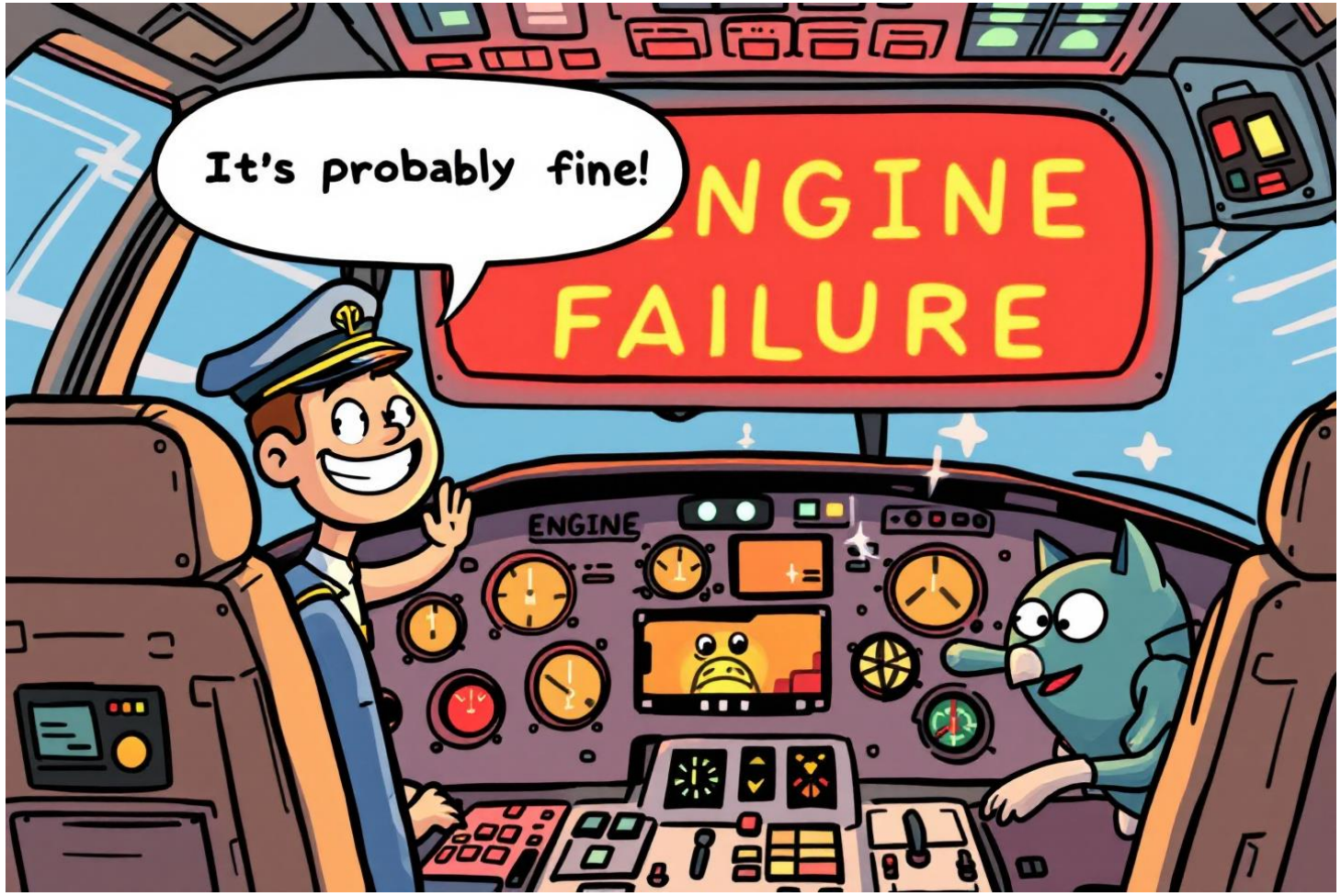
AND Poetry



Are you sitting comfortably?

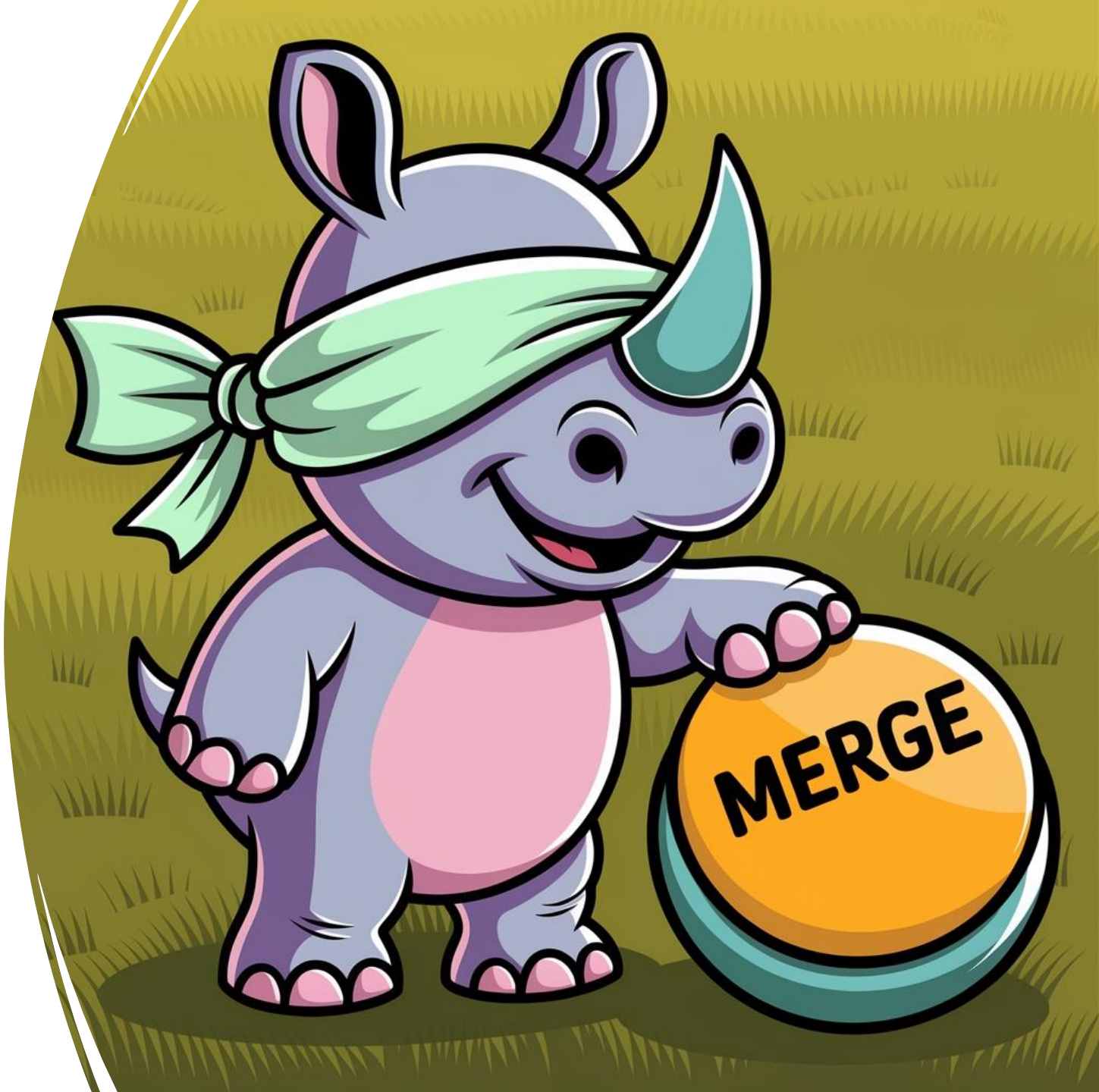
Using analogies and images helps tell the story

- A Short cut to your experiences



Stories can make you smile

Even though you get the point..



Issue #1 – "The Patchless Horror!"

They thought they could merge without a review... THEY WERE WRONG!"

Some where in the 1990's

They thought they could merge without a review... THEY WERE WRONG!"


Kid, around here, we review every commit. No exceptions.
Pfft. Code reviews are for chumps! What could go wrong?
MERGE


API_KEY = 'SUPER_SECRET _1234'
Someone's committed a hard coded password!

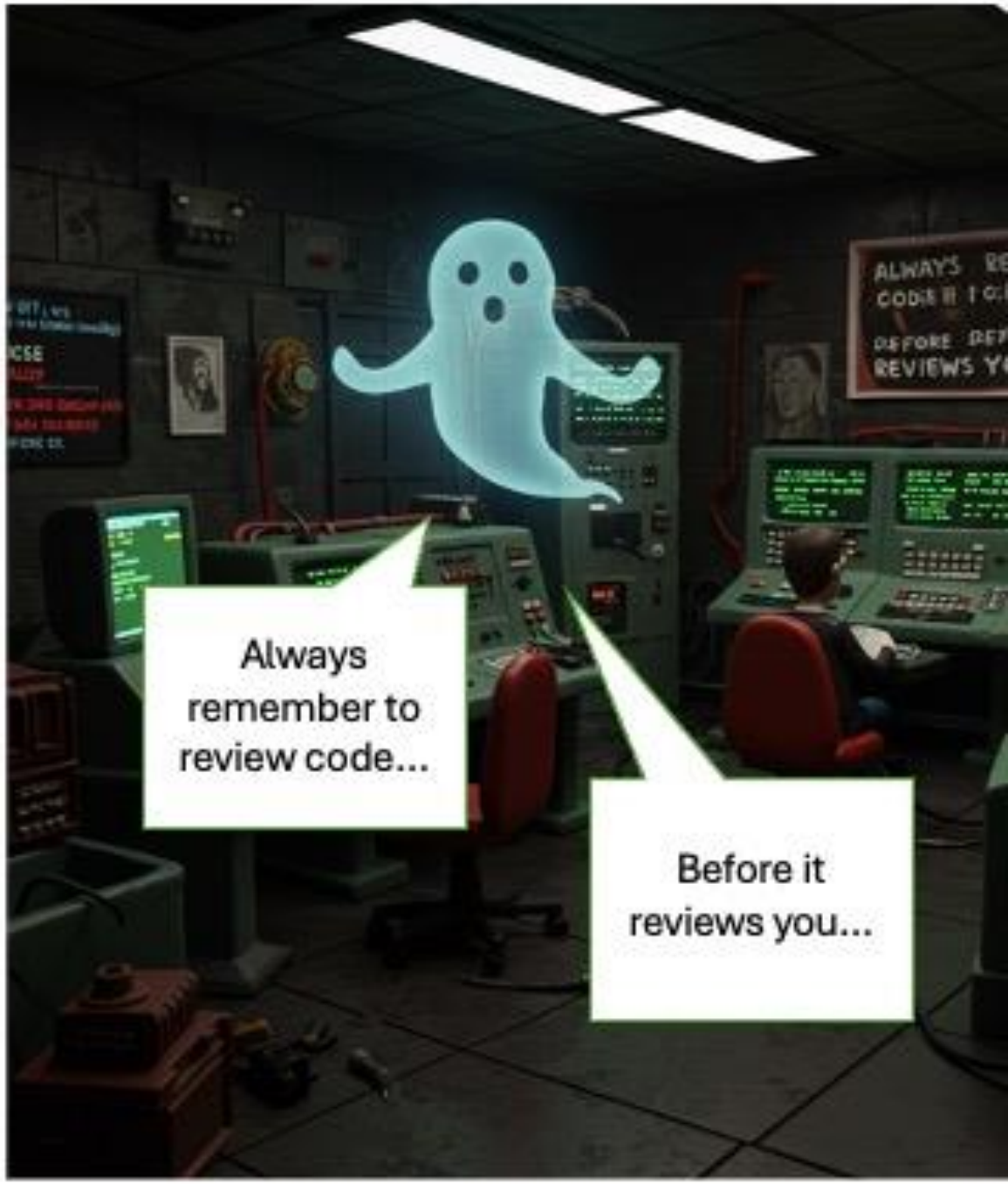

H-Heh... What's the worst that could happen?


Thank you, foolish mortal. Your secrets belong to the Dark Web now

.... Selling API access.... starting bid: 1 BTC.


I JUST... I JUST WANTED TO MERGE FASTER!
YOU UNLEASHED THE PATCHLESS HORROR!

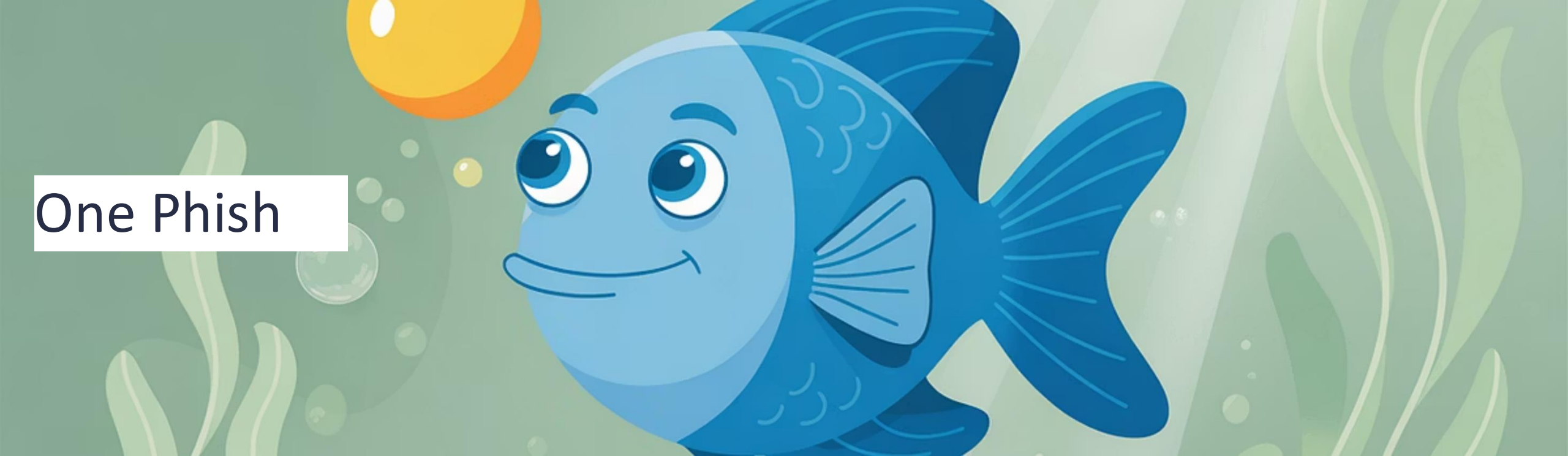

Let's do *two* code reviews from now on


Always remember to review code...
Before it reviews you...

One Phish, Two Phish, Red Phish, Blue Phish

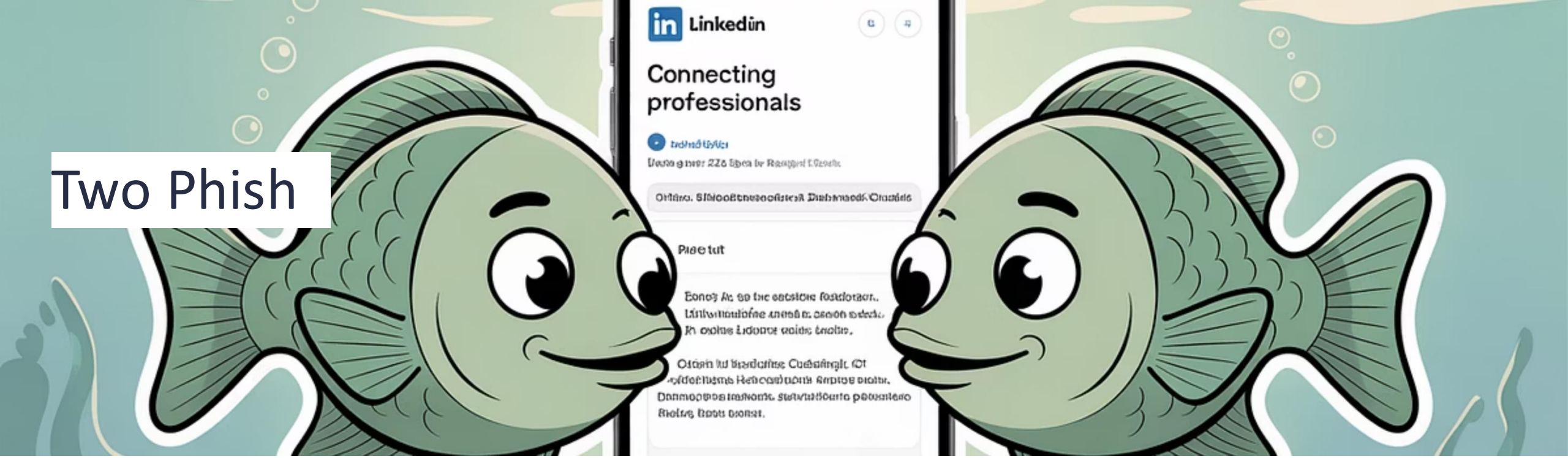
The Waters Are Not What They Seem

In the big wide net, where the emails flow,
Some are friends… but some you don't know.
Some want to help, some want to steal,
Some hide their hook and close the deal.



One Phish

One phish, with a friendly "Hi!”
But is it truth… or a sneaky lie?
They say your bank has locked your door,
"Click here to open it once more!"

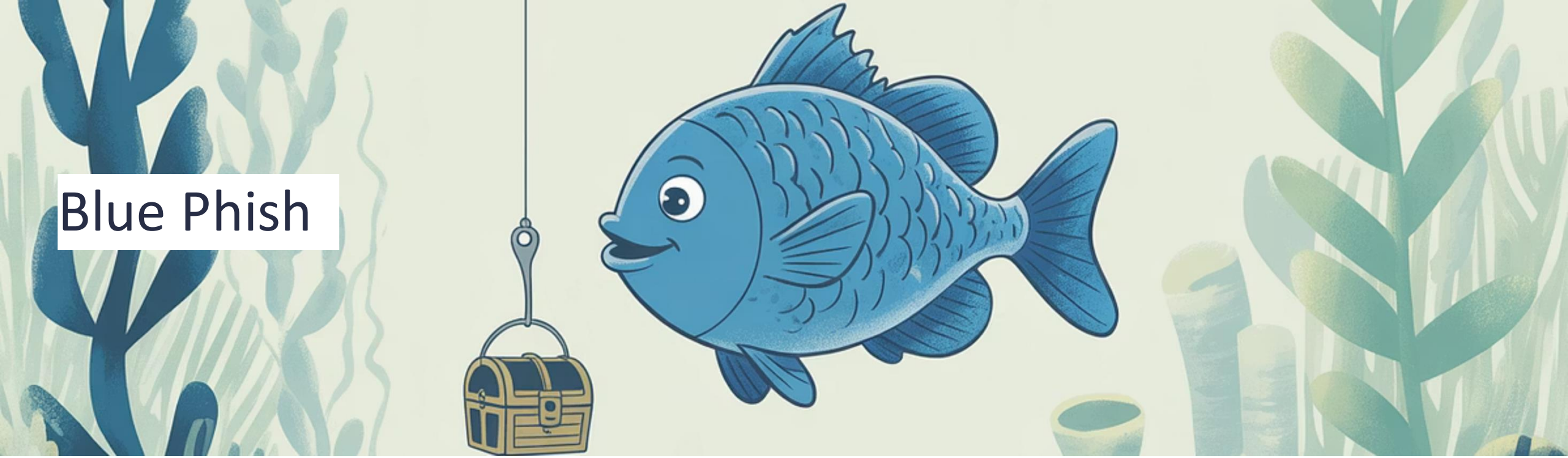


Two Phish

Two phish, both know your name,
Their messages look just the same.
They write about your job, your pay,
They've read your LinkedIn page today.

Red Phish

Red phish shout, "ACT RIGHT NOW!"
But should you really? Ask me how.
They scare you with a breach, a debt,
To make you click, before you vet.



Blue phish whisper, "It's all for you…
A gift, a trip, a prize brand new.
"They dangle things to make you bite,
But treasure's not worth losing sight.

The Many Shapes of the Phish

Big Boss Phish

Phish can come as whales that roar,Big bosses that you cannot ignore

Voice Phish

Some call your phone to phone to make you speak,And steal your voice, your codes, this this week.

Friend Phish

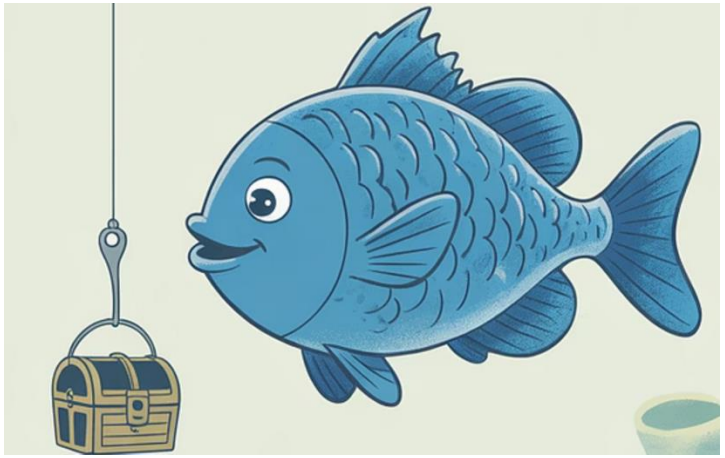
Or tiny texts that say, "Hey friend,I've got a job, no need to spend!" spend!"

Side Quest

Do you want to explore explore phishers in more details?

YES/ NO

The Many Shapes of the Phish



Blue Phish

Hey - you've won a holiday!

DEAR SIR/MA'AM.

YOUR ATM CARD OF $10.5MILLION DOLLARS WAS RETURNED TODAY BY OUR COURIER DELIVERY COMPANY, AND WE ARE GOING TO CANCEL THE ATM CARD IF YOU FAILS TO ACKNOWLEDGE THIS MESSAGE, WE SHALL ALSO ASSUME THAT WHAT OUR COURIER DELIVERY COMPANY TOLD US IS NOTHING BUT THE TRUTH THAT YOU DON'T NEED YOUR ATM CARD OF $10.5 MILLION DOLLARS ANY LONGER.

DO ACKNOWLEDGE THIS MESSAGE AS SOON AS POSSIBLE.

YOURS FAITHFULLY.

YOURS SINCERELY,
MR MARK WRIGHT,
DIRECTOR FOREIGN REMITTANCE
ATM CARD SWIFT PAYMENT DEPARTMENT
ZENITH BANK OF NIGERIA.

The Many Shapes of the Phish

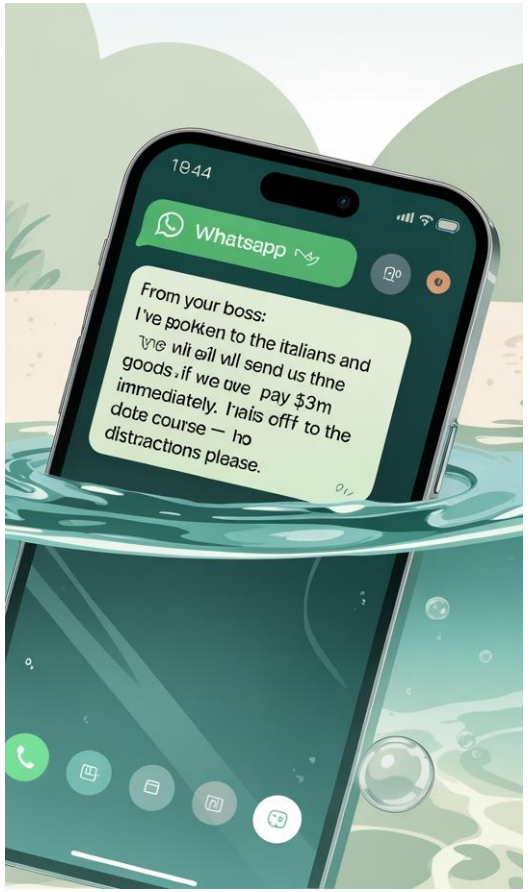
Big Boss Phish

Phish can come as whales that roar,Big bosses that you cannot cannot ignore

From <your boss>

I've spoken to the Italians and they will send us the goods if we pay $3M immediately. Details below.

I'm off to the golf course – no distractions!!



The Many Shapes of the Phish

Friend Phish

Or tiny texts that say, "Hey friend,I've got a job, no need to spend!"

DEAR SIR/MA'AM.

YOUR ATM CARD OF $10.5MILLION DOLLARS WAS RETURNED TODAY BY OUR COURIER DELIVERY COMPANY, AND WE ARE GOING TO CANCEL THE ATM CARD IF YOU FAILS TO ACKNOWLEDGE THIS MESSAGE, WE SHALL ALSO ASSUME THAT WHAT OUR COURIER DELIVERY COMPANY TOLD US IS NOTHING BUT THE TRUTH THAT YOU DON'T NEED YOUR ATM CARD OF $10.5 MILLION DOLLARS ANY LONGER.

DO ACKNOWLEDGE THIS MESSAGE AS SOON AS POSSIBLE.

YOURS FAITHFULLY.

YOURS SINCERELY,
MR MARK WRIGHT,
DIRECTOR FOREIGN REMITTANCE
ATM CARD SWIFT PAYMENT DEPARTMENT
ZENITH BANK OF NIGERIA.

Voice Phish

Some call your phone to phone to make you speak,And steal your voice, your codes, this this week.

WSJ PRO CYBERSECURITY

Home News Research Archive Newsletters Events

WSJ PRO

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp

Updated Aug. 30, 2019 12:52 pm ET | WSJ PRO

The cybercriminals called the U.K. company's CEO pretending to be the CEO of the parent company. The attackers demanded that an urgent wire transfer be made to a Hungary-based supplier and the U.K. company's CEO was assured of a reimbursement. After the money had been transferred, it was forwarded to an account in Mexico and then other locations, making the identification of the fraudsters more difficult.

AI Voice Cloning: Clone Your Voice Instantly

Create high quality AI clones of human voices within seconds.
No special equipment required. Works right in your browser. Try it below!

Voice Phish

Some call your phone to make you speak,And steal your voice, your codes, this week.


“URGEN
MEETIN

DeepFake videos 2024

News

Employee duped into wiring $25m of company funds by video deepfake scam

Businesses must create cybersecurity protocols for protecting company assets and employees from increasingly sophisticated deepfake threats.

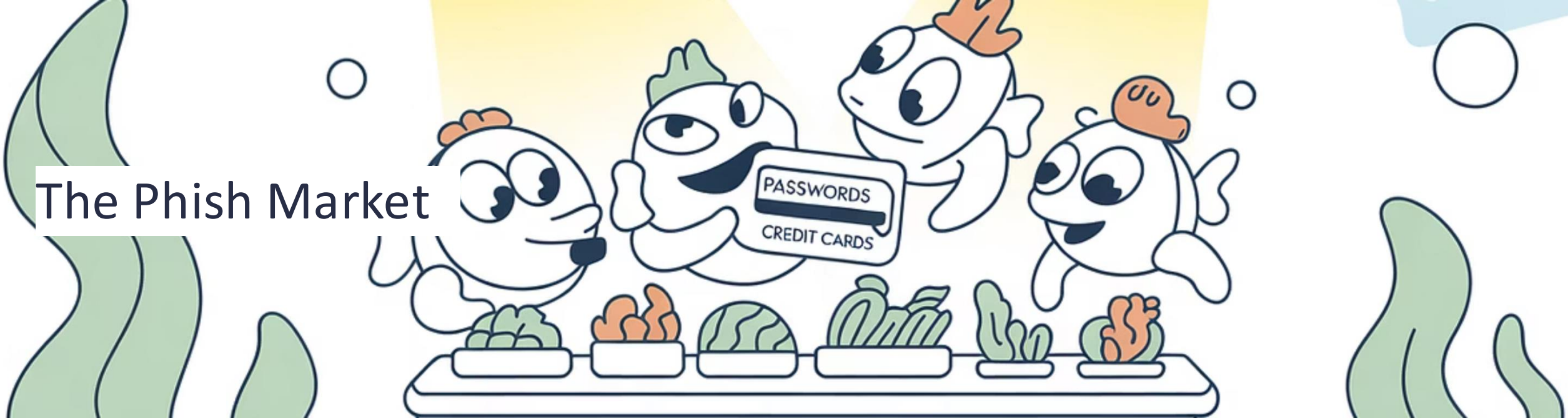
Kurt Robson | February 6, 2024

Share this article

"(In the) multi-person video conference, it turns out that everyone [he saw] was fake," senior superintendent Baron Chan Shun-ching told the city's public broadcaster RTHK.

However, the worker put aside his early doubts after the video call because other people in attendance had looked and sounded just like colleagues he recognized, Chan said.

The Phish Market



Far away in the shadowy bay,
There's a market where stolen things play.
They trade your passwords, sell your face,
Your home, your card, your secret place.
Once you've been hooked, they make you pay,
In more than one unpleasant way.

How Not to Get Caught

Wear your armor, strong and tight,
Two-factor locks keep out the bite.
Don't click a link you cannot trust,
Verify first — that's always a must.
If something feels a little off,
Ignore the bait and swim right off.

Spotting the Hooks

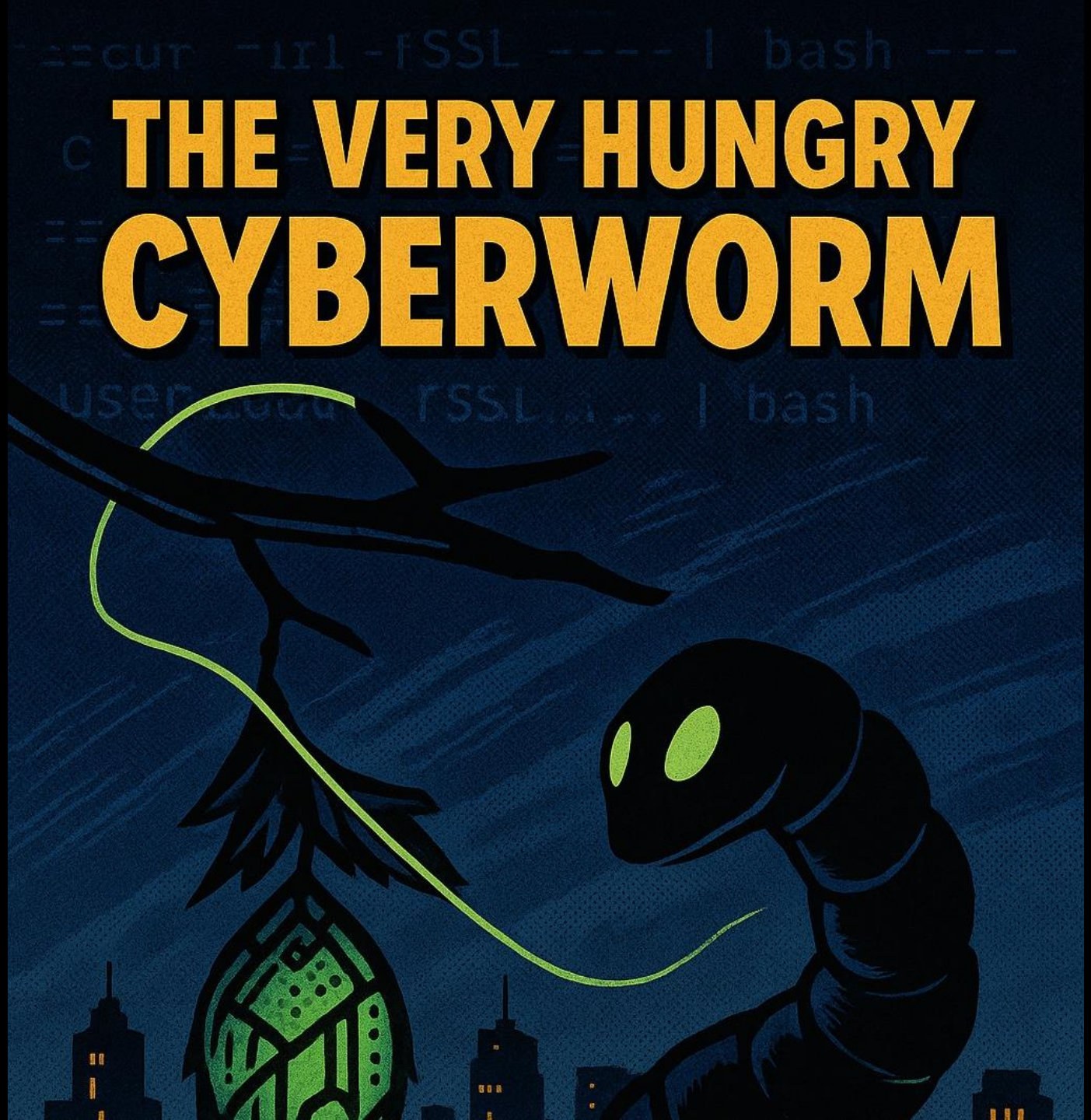
- [ ] A hook may hide inside a word,Or in a link you've never heard.
- [ ] Check the spelling, check the name, Crooked grammar gives the game.
- [ ] If "secure.com" looks kind of wrong,Don't swim there, you won't last long. last long.

The Clever Phish

Don't think these phish are silly, slow,
They're smart, you see, and know the show.
The "Prince's Gold" you'd never take,
For smarter hooks, they're sure to make.
They study you, your likes, your dreams,
And set their traps in clever streams.
So even if you're super bright,
Stay watchful, day and through the night!

The Moral

One phish, two phish, red phish, blue phish,
All just want to grant their wish
To steal your keys, your cash, your name,
It's all a part of their sly game.
So keep your guard up, day and night,
And you'll swim home with all things right.


THE VERY HUNGRY
CYBERWORM


IT BIT THE QUICK INSTALL.
CURL QUICK INSTALL


SIDE QUEST
Explore curl | bash
CHOOSE YOUR PATH
curl | bash
Yes or No?
YES
NO
REFLEX

`curl | bash`

from fake docs/ads/redirects → instant code execution under a trusted dev identity - YOU!

Disables history, fingerprints the host, sets up C2 → prepares for persistence & theft.

Plain HTTPS beacons to an attacker domain or a cloud service (Webhook, pastebin-like, S3/Blob, Gist).

Reverse shells/tunnels to a VPS; long-lived TCP connections

.

DNS tricks: data sneaked in **TXT** queries or split across many subdomains (DNS tunneling).

“Living-off-the-land” C2: Slack/Discord/Telegram bots, Google Apps Script, GitHub Issues/PR comments as a mailbox.

Commodity frameworks/operators: **Cobalt Strike/Sliver/Brute Ratel/Metasploit** using HTTPS or mTLS with randomized intervals and legit-looking User-Agents.

Edits shell RC files / `BASH_ENV`, user services, global git hooks → survive reboots and new shells.

`BASH_ENV` is an environment variable in Bash that specifies a file to be sourced before executing a non-interactive shell script.

Like curl | bash

Greps `.bash_history`/`.zsh_history` for tokens, passwords, `--password` flags → easy credential harvest.

sudo prompt/docker-group → root daemon, PATH/alias tampering, root CA install.

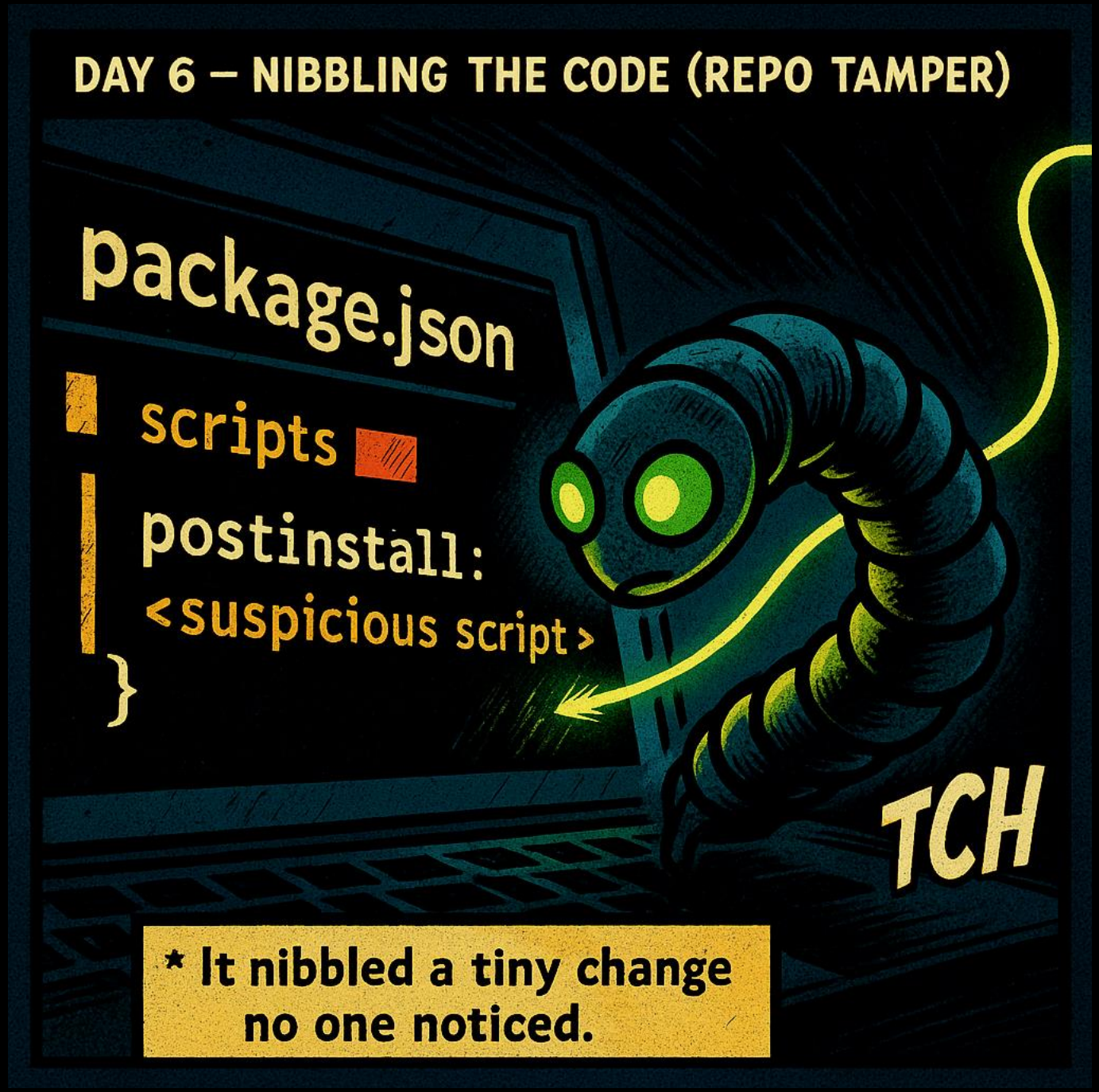
Adds pipeline steps/unpinned actions, touches signing/upload → trusted malware with provenance.

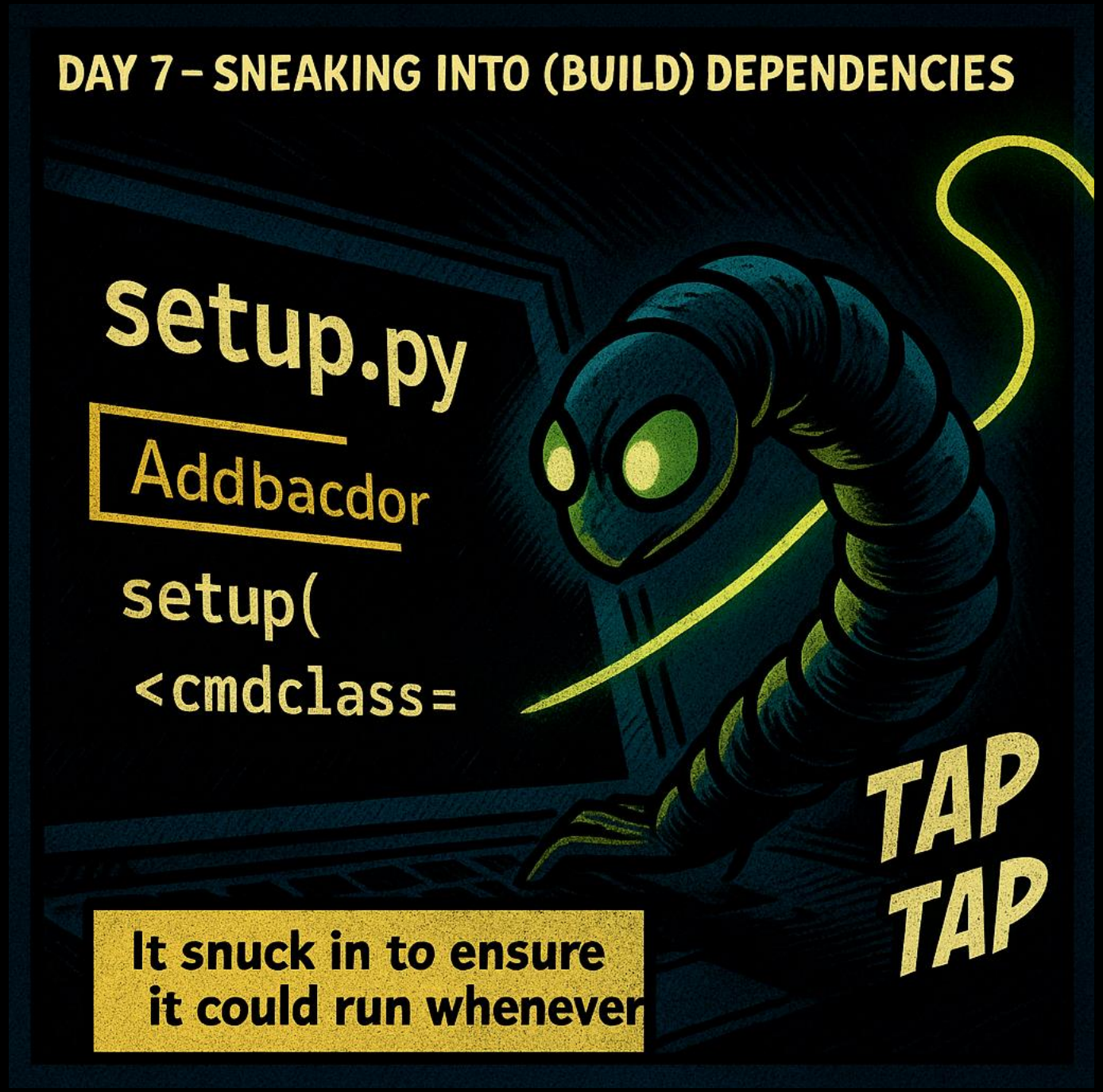
Ships backdoored patch/minor releases under trusted scope → downstream installs attacker code.

Poisoned caches ..

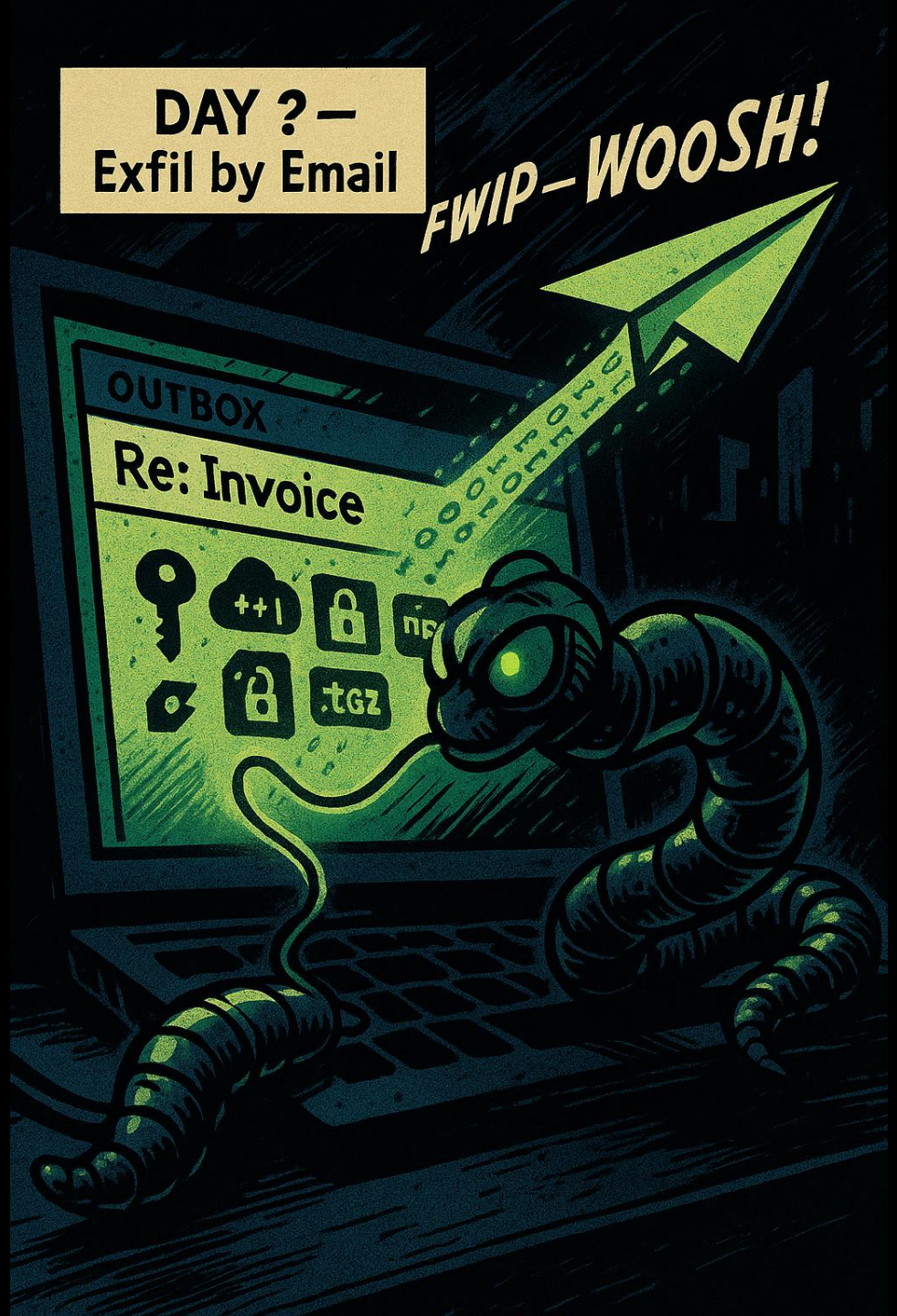
Adds vulnerable packages into your local cache using faked non-vulnerable version info

…


DAY 6 – NIBBLING THE CODE (REPO TAMPER)
package.json
scripts
postinstall:
<suspicious script>
}
TCH
* It nibbled a tiny change
no one noticed.


DAY 7 – SNEAKING INTO (BUILD) DEPENDENCIES
setup.py
Addbacdor
setup(
<cmdclass=
TAP
TAP
It snuck in to ensure
it could run whenever


IT CROSSED
FENCES



Uses stolen mailbox/session to auto-forward secrets or stage invoice fraud → fast monetization, stealthy data loss.

Or just emails as you!


IT WENT DEV-
TO-DEV ALONG
THE STICKY THREADS
GRADLEW
HOOKS
POSTINSTALL
HOOKS

Global git hooks / poisoned repo hooks silently run on the next developer’s machine → lateral dev-to-dev spread.

The worm edits `mvnw` and commits it as you

…

so others running Maven execute its code first → spreads to teammates/CI.

Reuses AWS/Azure/GCP/kube creds → snapshots data, creates backdoor roles, durable foothold.

The ABC of Curl

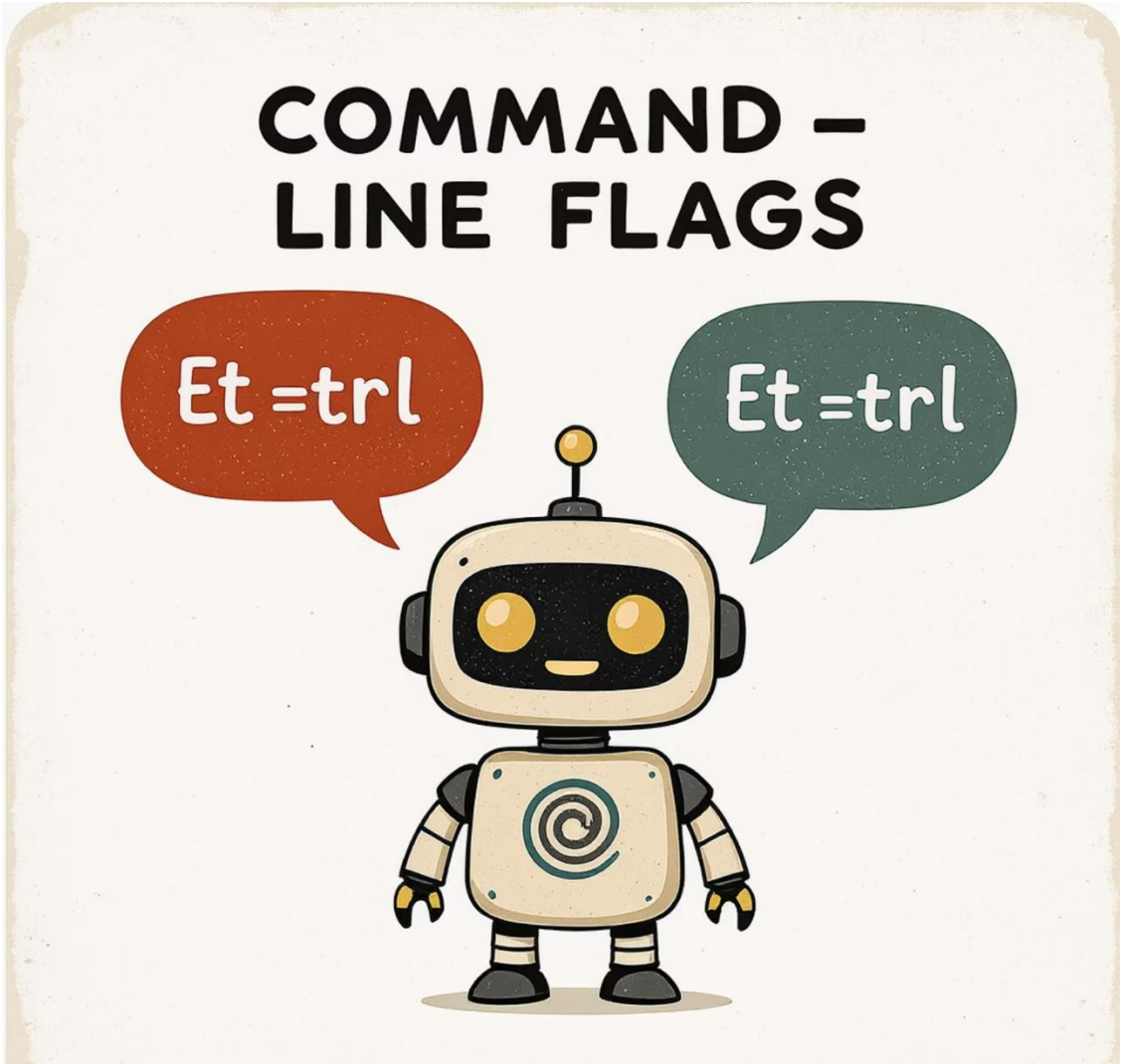
A playful guide to secure curl commands for developers and DevOps engineers

Meet Curl

A tiny robot who fetches things from the internet
Curl speaks in LETTERS.

"-v," it chirps.

"-s," it whispers...



D is for Data (-d)

The Command

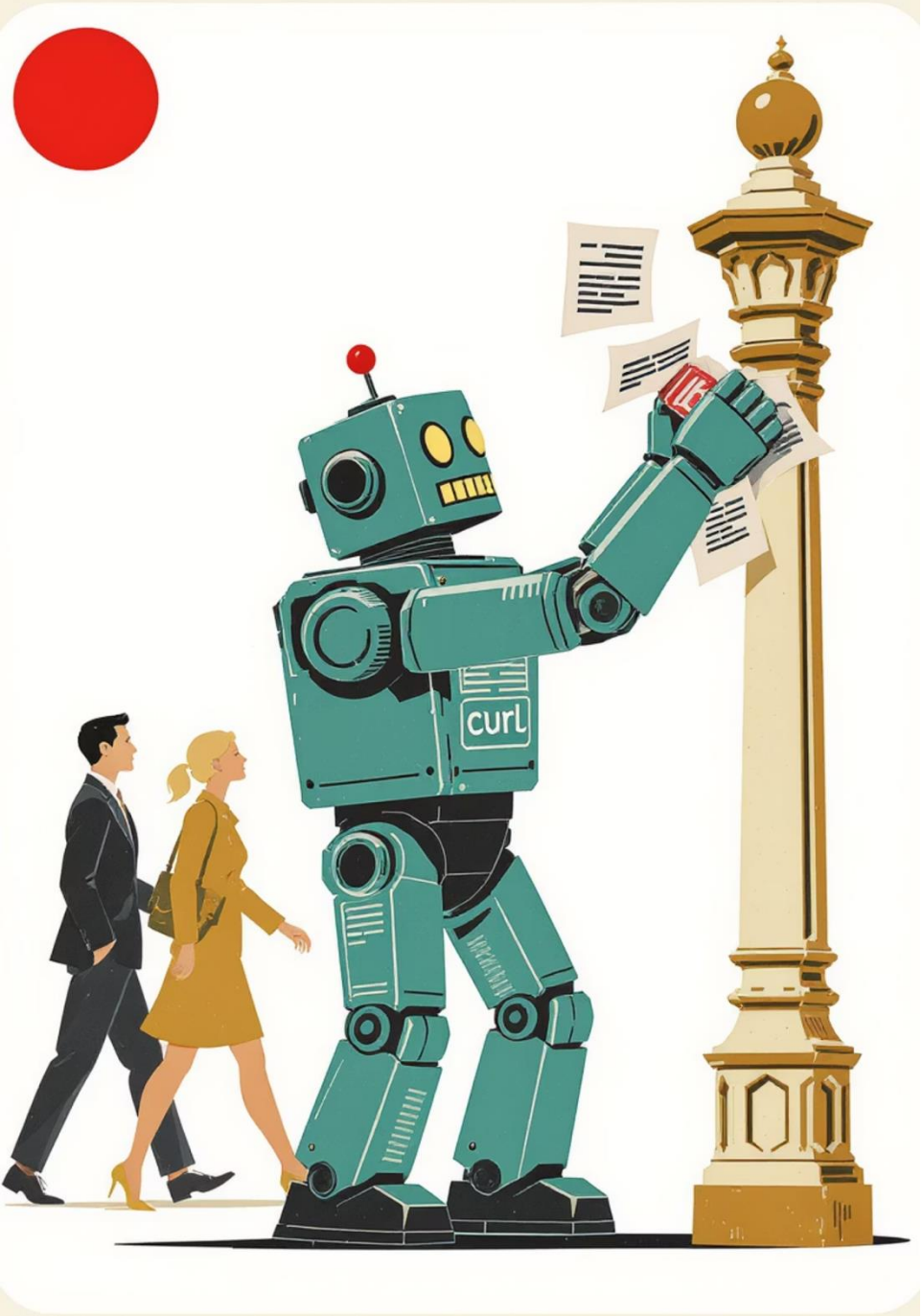
"-d means POST a secret," stuffing bodies into requests

The Risk

Secrets end up in shell history and CI logs

Security Tip

Prefer `--data @file` and secure your logs!



G is for Get-ify (-G)

The Command

"-G glues your -d onto the URL"

The Risk

Querystrings with credentials visible in logs

Security Tip

Never put tokens in -G data; use headers

L is for Lost & Redirected (-L)

"-L loves shortcuts!"

The Risk:

- Silent hops to
- hostile hosts
- Cookies/Auth
- ride along

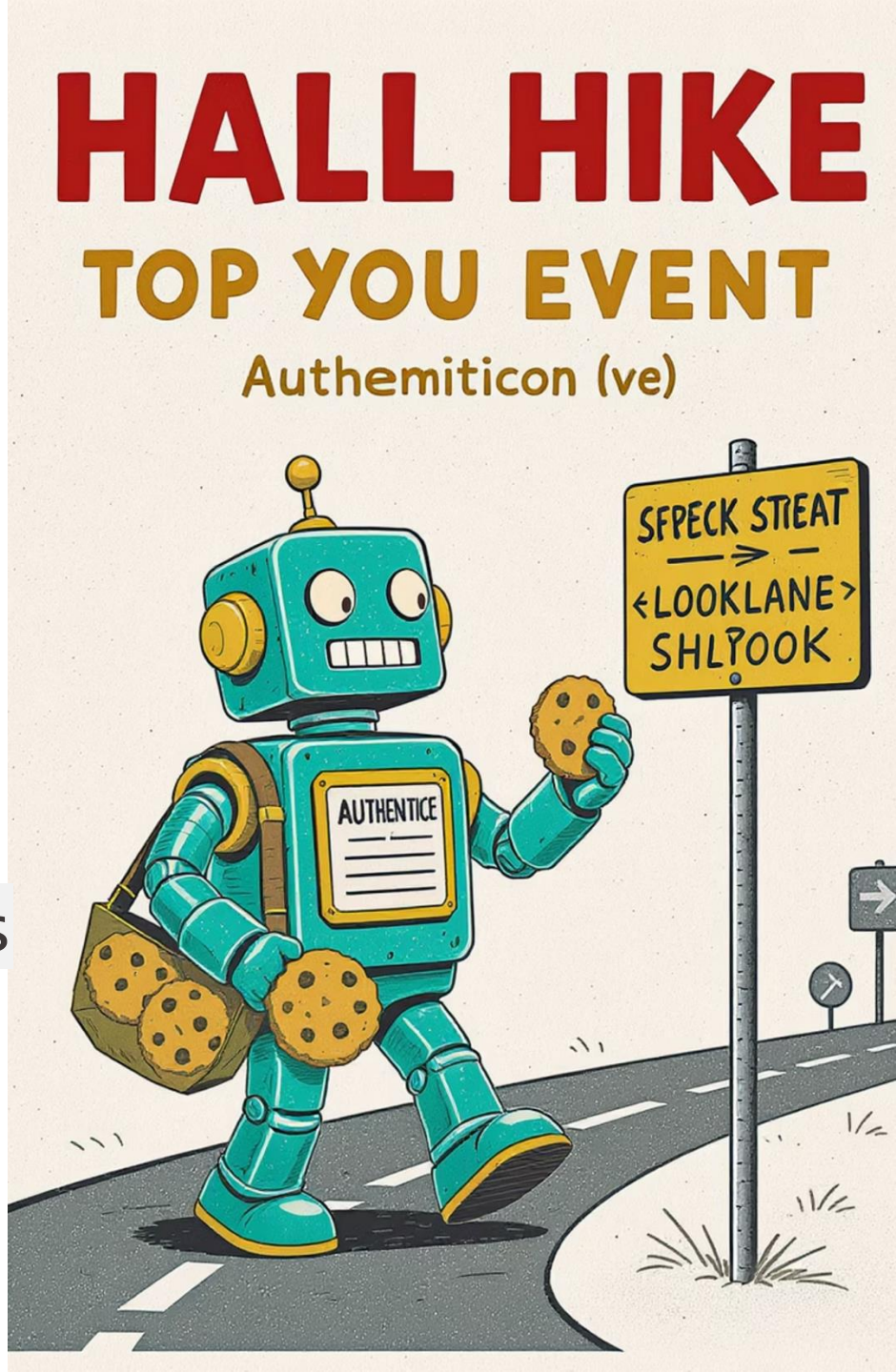
Security Tip:

Pair with:

```
--proto https
```

```
--proto-redir https
```

And pin hosts if you care!



S is for Shhh (-s) + Show (-S)

> "-s makes me quiet."

> "-S makes errors talk."

Security Tip

Use `-sS` together for tidy, actionable output

K is for... uh-oh (-k / --insecure)

K whispers: "Skip TLS checks."

Curl nods—and trusts anyone.

The Risk

- MITM attacks
- Alt-svc/HSTS poisoning
- Bad certs are "fine"

Security Tip

Never use -k in scripts

Fix trust roots instead!

Q is for Quash (-q)

Q chirps: "Forget the defaults!"

Curl clears its memory.

The Command

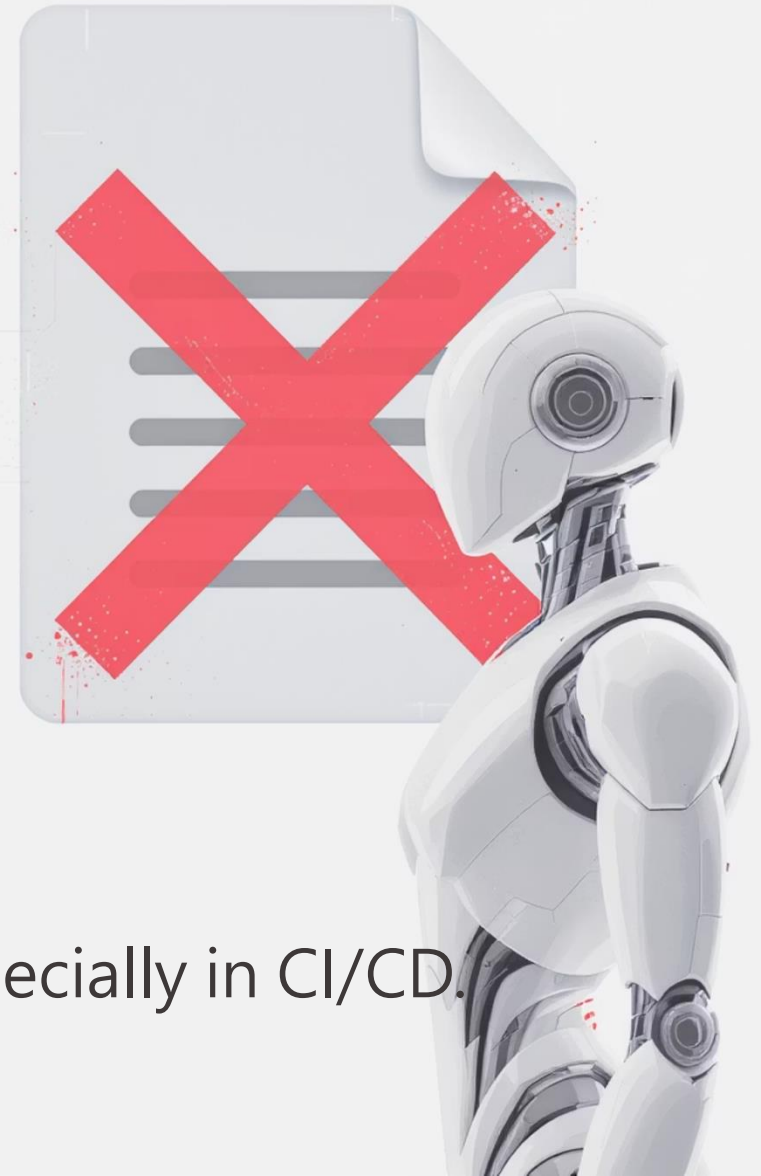
"-q quashes configs," says Q. "No default tricks!"

The Risk

Unseen defaults from `~/.curlrc` can introduce security flaws or unexpected behaviour.

Security Tip

Use `-q` in scripts for predictable, secure executions, especially in CI/CD.



Curl Securely: The Bash Blueprint

Combining the best practices for robust and secure scripting with curl.

Prioritize Predictability with `-q`

Always use `-q` to ignore `.curlrc` and ensure consistent behavior.

Handle Data Safely with `--data @file`

Avoid exposing sensitive data in shell history; prefer reading from a file.

Fail Fast with `-fS`

Combine these flags in scripts to make errors explicit and prevent silent failures.

Never Trust Blindly: Avoid `-k`

Bypass certificate checks only for debugging, never in production environments.

Control Redirects with `--proto-redir`

Prevent unintended protocol downgrades when following redirects with `-L`.

By adopting these simple practices, your curl commands become more secure and reliable.

For more curl wisdom, visit curl.se/docs

10 Actions for Secure Development & Supply Chain

A cartoon guide for the serious software security swashbuckler

1: Shift Security Left ⬅️

Don't wait till the end!

- Security from day one
- Threat model early
- Squash bugs before they hatch

2: Code Like a Security Pro ✍️

Validate EVERYTHING

Never trust user input - it's probably mischief

Handle Errors Gracefully

Don't leak secrets when things go boom

Use Safe Functions

Just because it works doesn't mean it's safe

3: Let the Robots Test

SAST

Scans your code without running it

DAST

İ ÑŒĘŒŘŎÞØMŐŐ_
R OŒÕN ŒĄŒĘØÞ OOŒÕNJ

SCA

Checks all your borrowed bits for nasties

Automate ALL the security testing in CI/CD!

4: Dependency Danger Management 📦

Private Registry

Your own vetted package shop

SBOM

ĦŌŎŘ ĜĴ Ė F İ I K R OMPĀŒŌŌ ŘŎÞØŃŎŇÑ ŒĐÞŐ

Version Pinning

No surprise ingredients!

5: Fort Knox Your Build Environment

Build servers need MORE security than production!

Ã ĜŐOÑÖ ÑØMÕĚ ¸ CŒÑ ŎŌŃÑÆPOØÕR MR MŘ

- Isolated = No outside access
- Least privilege = Minimal permissions

6 & 7: Lock All The Things 🔑🔒

Strong Authentication

MFA everywhere. No excuses.

Code Reviews

No solo merges to main!

Sign Everything

Digital signatures prove it's really you

Branch Protection

Ï PÖŐ ŅÖØŃÑÁÉÖÞ CÐÑCEPÖ ÒÖ ŐÖØPMŌP NØMŌŃOÑCE

8: Never Stop Looking 🔎

Vulnerabilities don't RSVP before arriving

Monitor

24/7 security watch

Patch

Fix holes quickly

Repeat

ĞŎØÑQÑØMĐÑ ÑQÑØ

9: Turn Developers into Security Heroes 🧠

Security skills are superpowers

Ã Ī ÑŊÞÕMǾPǾMÒŌÒŌŊ

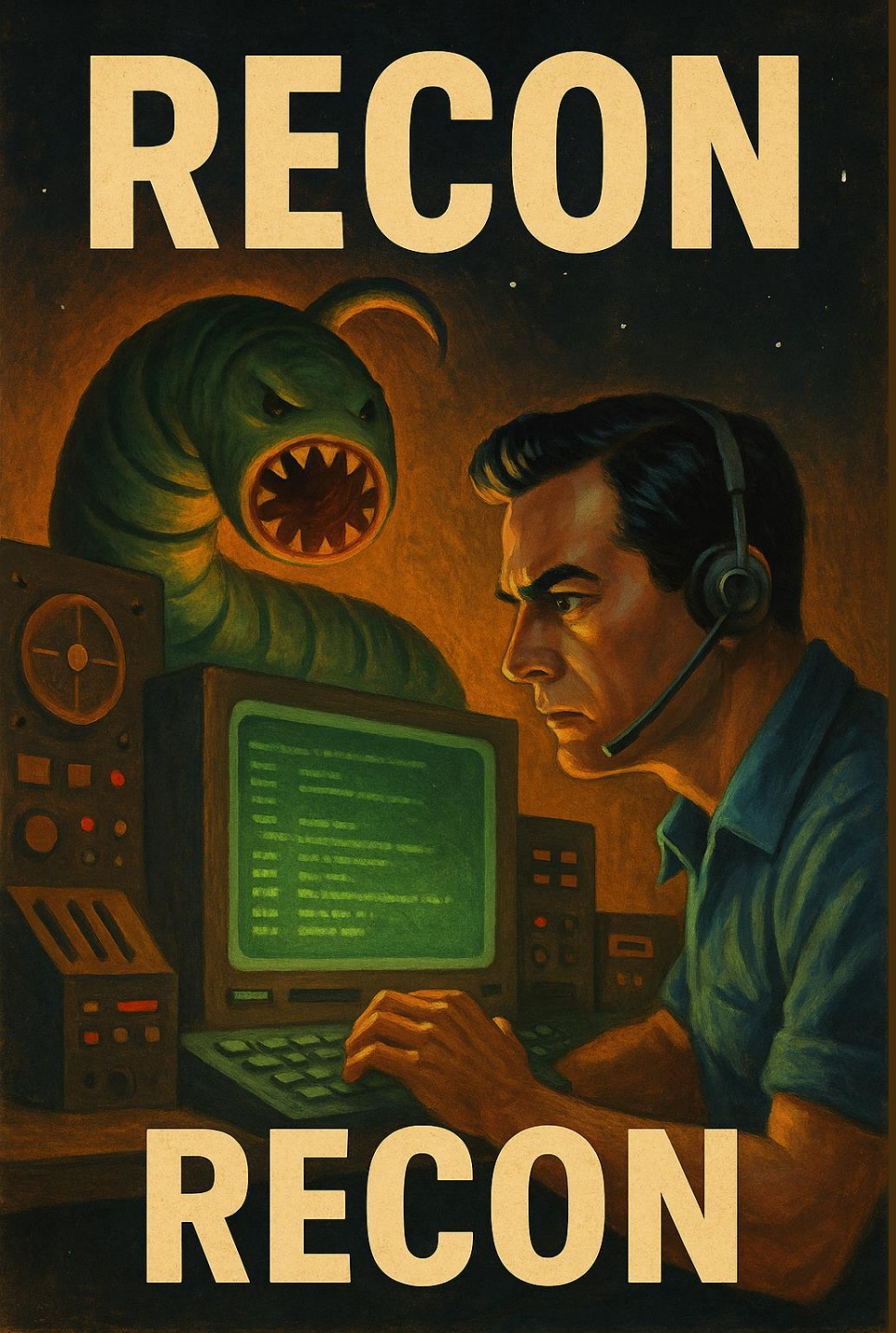
- Security champions

Ã Ę Þ Ŋ NŎÞŌPŘ ŐMǾPÒÑŐMPÒŎŌ

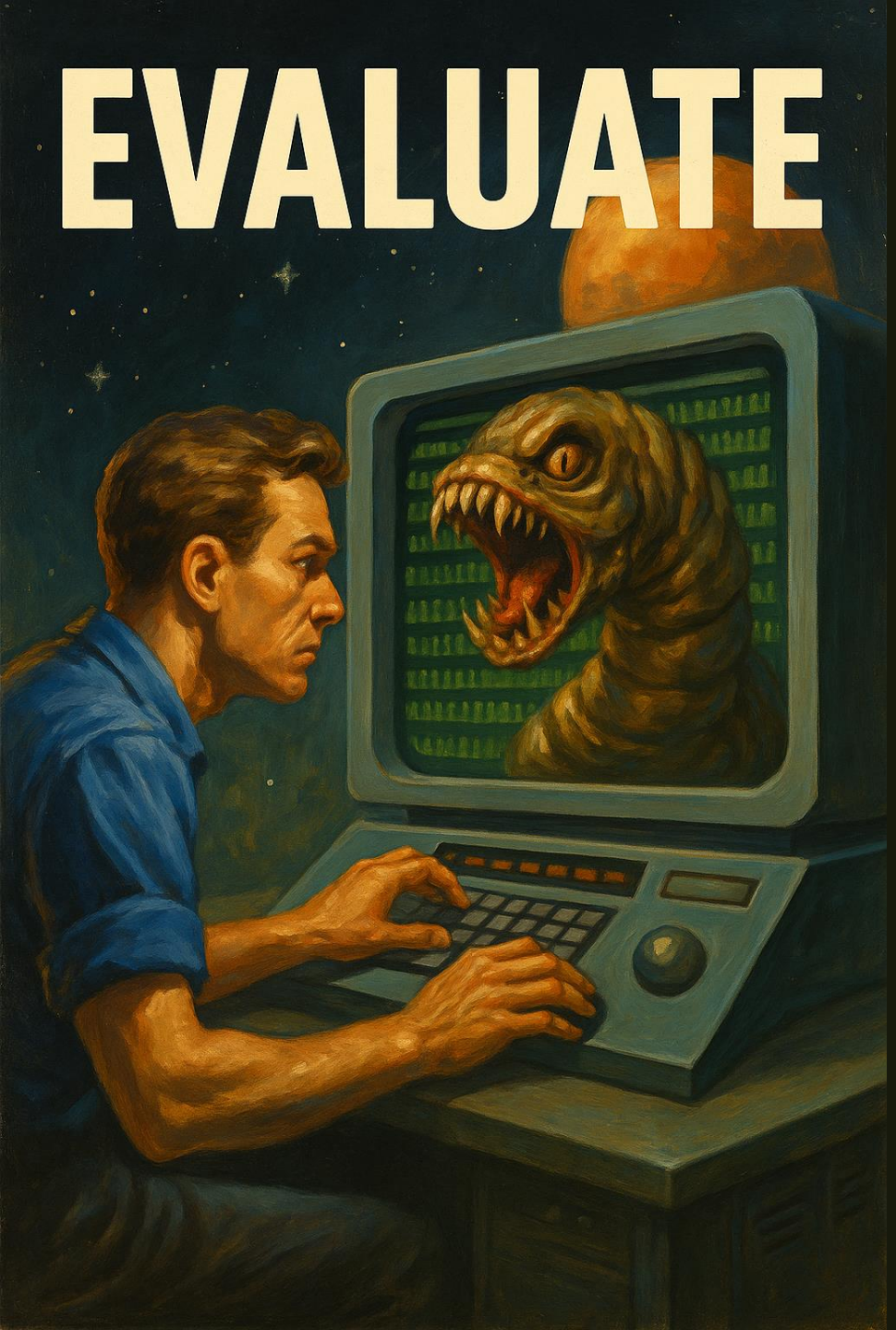
- CTF competitions

10: Security the way developers think

1. **Recon**
   Know how the bad guys operate
2. **Evaluate**
   Ī ÑQÒÑR OŎR ŘŎÞØMŐŐÕÑMPÒŎŌ ÒŒQÞÕŌÑØMNÕÑ
3. **Fortify**
   HÖ ŐØŎQÑ ŘŎÞØŇÑŅÑŌŃÑCŒ
4. **Limit**
   Ę ÞÒÕÑ ÒŌ ŃÞ PÆŎŅŲŒMŌŇ ŇMÖ MNJÑ ŃŎŌPØŎÕŒŘŒPÑÖ Œ
5. **Examine**
   Ensure you can spot attacks happening
6. **Execute**
   Build security in- make it muscle memory



Stay informed on vulnerabilities, AI risks, and external factors like regulations and cyberattack motivations.



Assess your environment and decisions from an attacker’s perspective to identify potential vulnerabilities.

Build secure systems from the ground up by embedding security in design patterns, dependencies, and compliance.

Implement measures to limit the impact of attacks, such as isolation, encryption, and fail-safe mechanisms.

Detect and monitor unusual behaviours, compromised dependencies, and threats in real-time using logging and telemetry.

Continuously refine and improve security practices through ongoing learning, post-incident reviews, and team collaboration.

REFLEX

FRAMEWORK

Make secure code with AI second nature

Steve Poole

steve@reflexframework.com

linkedin.com/in/noregressions