FIELD MANUAL · V1.0 · 2026

THE INSIDER'S OPSEC FIELD MANUAL

What Big Tech doesn't want you to know about protecting yourself online.

SNAYR
snayr.dev

TRANSMISSION RECEIVED · 02:47 AM

Listen carefully.

I work where the secrets are kept. AI models you'll never see. Threat reports that never reach the news. Settings buried so deep most engineers in the building can't find them.

I started this because someone I love almost lost everything to a phone call that lasted forty seconds. The voice on the other end belonged to her son. He was sitting next to me at the time.

The internet is not what they sold you. It's a marketplace, and you are inventory. This manual is the floor plan of that marketplace, with the cameras marked.

Read it once. Apply three things tonight. Send it to one person who needs it tomorrow. That's the deal.

— SNAYR

CONTENTS

What's in this manual

This is the public version. The full Field Manual — 100+ pages, quarterly updates, threat library — is at snayr.dev/manual.

01

CHAPTER ONE

The Voice on the Phone Isn't Theirs

One in ten Americans has been hit by an AI voice clone scam. Most don't realize it until the wire is gone.

CHAPTER 01 · VOICE CLONES

THREAT VOICE CLONE EXTORTION HIGH

How it works

Three seconds of clean audio is enough. A TikTok caption, a voicemail greeting, a wedding video uploaded to YouTube — that's the training set. The cloning model runs in under a minute. By the time the call comes in, the script has been generated by a second AI that scraped your family's public footprint to find leverage.

> ! **The trap is built around your life.** They know the school. The friend's name. The trip last weekend. The "kidnapper" sounds informed because they are.

The three signs you're being cloned

01 **Background is too clean.** Real distress calls are loud, breathless, chaotic. AI generation often has unnatural silence between phrases.

02 **Same emotional pitch throughout.** Real fear escalates and crashes. Cloned audio plateaus.

03 **Refusal to answer specifics.** Ask one thing only your real person would know. The AI will deflect, repeat the script, or claim the kidnapper is listening.

CHAPTER 01 · VOICE CLONES

The Defense Protocol

01

Set a memory key

Not a password. A shared memory question only the two of you would know, that's not online anywhere. Test it this weekend.

02

Lock the audio

Strip audio from public posts. Set Instagram, TikTok, YouTube to private — at minimum for everyone under 25 in your family.

03

Hang up. Call back.

The rule that stops 95% of these. If the call sounds wrong, hang up. Call them back on the saved number. Always.

> AI can clone the voice. It cannot clone the relationship. That's the gap they can't cross.

THE RELATIONSHIP IS THE UNFORGEABLE SIGNAL.

02

CHAPTER TWO

Your Phone Knows. Tell It to Stop.

Twelve toggles, ten minutes. Seventy percent of your data exposure disappears.

CHAPTER 02 · PHONE PRIVACY

EXPOSURE DEFAULT TRACKING MEDIUM

The defaults are not for you. They are for the advertising engine, the carrier, the data broker, and the dozen apps that paid for placement. Walk through this once. You won't need to do it again for a year.

iPhone — the twelve toggles · part 1

01 Settings → Privacy → Tracking
Disable "Allow Apps to Request to Track"

02 Settings → Privacy → Apple Advertising
Disable "Personalized Ads"

03 Settings → Privacy → Analytics & Improvements
Disable "Share iPhone Analytics"

04 Settings → Privacy → Location → System Services
Disable "iPhone Analytics", "Routing & Traffic", "Significant Locations"

05 Settings → Cellular → Cellular Data Options
Enable "Limit Precise Location" (iOS 26.3+, supported devices only)

06 Settings → Safari → Privacy & Security
Enable "Prevent Cross-Site Tracking" + "Hide IP Address"

iPhone — the twelve toggles · part 2

07 Settings → Mail → Privacy Protection

Enable "Protect Mail Activity"

08 Settings → Notifications → Lock Screen

Hide previews — set "Show Previews" to "When Unlocked"

09 Settings → Privacy → Microphone & Camera

Audit per-app — revoke any app you don't actively trust

10 Find My → Me → Share My Location

Disable, OR limit to two trusted people only

11 Settings → General → Background App Refresh

Disable for everything except messaging

12 Settings → Wi-Fi → Edit (each network)

Enable "Private Wi-Fi Address" + "Limit IP Address Tracking"

i

Android: most equivalents live under Settings → Privacy and Settings → Security. The toggle that stops AirTag stalking is at Settings → Safety & Emergency → Unknown Tracker Alerts. Turn it on tonight.

03

CHAPTER THREE

The Inbox is the Front Door

Forty percent of phishing emails are now AI-written. You can't tell them apart anymore. So change the locks.

CHAPTER 03 · INBOX

THREAT AI PHISHING · 14× SURGE HIGH

The grammar errors are gone. The "urgent invoice" is from your real vendor's domain. The CEO's voice memo attached to it is real-sounding. You can't out-read this. You out-architect it.

The Three-Inbox System

Stop using one email address for everything. Split your life into three identities. The inboxes don't know about each other.

VAULT

Banks · Investments · Government

- Used for nothing else, ever
- 2FA via hardware key (YubiKey)
- Never shared, never typed in public
- One device only — your most secure phone

LIFE

Real friends · Real services · Subs

- 2FA via authenticator app
- Aggressive spam filtering
- Reviewed weekly, archived ruthlessly
- Never used for shopping or signups

BURN

Stores · Forums · One-time signups

- You expect this one to leak
- Hide My Email or SimpleLogin aliases
- No payment info ever attached
- Burn and replace every 18 months

CHAPTER 03 · INBOX

Five Triage Rules · Every Email, Always

01 **Hover, don't click.** Real link previews tell you the truth. Mismatched domains end the conversation.

02 **Urgency is the tell.** No legitimate institution makes you decide in fifteen minutes. Slow it down.

03 **Attachments before context.** If the body says nothing but "see attached", treat the attachment as live ammunition.

04 **Type the URL yourself.** Banks, gov, payroll. Always. Never click "log in" from the email itself.

05 **Confirm sideways.** Got a strange request from someone real? Text them. Different channel. Confirm before acting.

Tonight's drill: sign up for haveibeenpwned.com. Enter your VAULT and LIFE email. See every breach you're already in. Enable notifications. Free.

> Architecture beats vigilance. Vigilance fails on a tired Tuesday. Architecture works while you sleep.

04

CHAPTER FOUR

Passwords Are Liabilities, Not Assets

Your password leaked an average of 4.7 times. Stop trying to remember things. Start architecting your way out.

CHAPTER 04 · PASSWORDS

EXPOSURE CREDENTIAL REUSE HIGH

The password you use everywhere has been in at least one breach. Probably six. Attackers don't guess your password — they buy a list and try yours against four hundred other sites in the time it takes you to make coffee. This is called credential stuffing. It works because you're human, and humans reuse.

The Stack You Need

TIER 1 · BASELINE

Password Manager

1Password, Bitwarden (free), or Apple Passwords. One master password you actually memorize. Everything else: random, unique, generated. Non-negotiable.

TIER 2 · AMPLIFIED

Authenticator App

Aegis (Android), Raivo (iOS), or 1Password's built-in. Replaces SMS-based 2FA for everything that matters. SMS is broken — SIM swap attacks bypass it in twenty minutes.

TIER 3 · HARDENED

Hardware Key

YubiKey 5C NFC. Two of them — one daily, one in a safe. Plug into your VAULT email and primary banking. From this point forward, phishing-resistant. No software bypass exists.

Migration Path · Three Weekends

W1

Install + Master

Install Bitwarden or 1Password. Set strong master passphrase (4 random words + numbers). Enable biometric unlock.

W2

Migrate top 25

Email, banking, social, work. For each: log in, change to generated password, save. Don't try to do all 200 accounts. Top 25 covers 95% of risk.

W3

2FA + hardware

Enable authenticator-app 2FA on top 25. Order YubiKey. Enroll YubiKey on VAULT email + bank. Stash backup key in a safe.

> Strong passwords are an old idea. Strong architecture is the new one. Move the trust out of your head and into a system that doesn't sleep.

05

CHAPTER FIVE

When You Already Got Hit

The first hour determines the next year. Here's the order of operations when something goes wrong.

CHAPTER 05 · INCIDENT RESPONSE

RESPONSE INCIDENT TRIAGE CRITICAL

Most damage in a compromise happens in the first 60 minutes — before the victim even knows. The second wave hits when they panic and click the "fix it" link in the warning email. Use this order. Memorize it.

The First Hour · In Order

T+0

Disconnect

If a device is acting wrong, take it off the network. Airplane mode + Wi-Fi off. If laptop: pull the cable, disable Wi-Fi. Buys you time before exfiltration completes.

T+5

Change passwords from a CLEAN device

Different phone, different laptop, different network. In order: primary email first, then banking, then social. Use the password manager. Force log-out of all sessions on each.

T+15

Freeze credit

In the US: Equifax, Experian, TransUnion online forms — 5 minutes each. Free. Locks lenders from issuing new credit in your name. In Poland: BIK alert, then individual bank notification.

The First Hour · continued

T+30

Notify your bank · in person or via app, never via call

The fake "fraud department" call is the second wave. Use your bank's official app to message support, or walk into a branch. Never call back numbers from email or text.

T+60

Document everything

Screenshots. Email headers. Times. Amounts. You'll need this for police, insurance, bank disputes, and tax filings. Write it down before memory fades.

!

Things you do NOT do: click any "your account is secured, log in here" emails. Call any number from a text. Send money to "recover" stolen money. Pay ransom for "deleted files". Reset from a backup that includes the compromised period.

06

CHAPTER SIX

The Family OPSEC Codex

Your security is the strength of your weakest household member. Here's how to harden everyone — without sounding paranoid.

The four conversations to have this month

01

Memory key with parents

The voice clone scam targets parents first. Set a memory question they can answer under pressure. Practice it once, calmly, this weekend. Tell them: any call asking for money, hang up and call back on the saved number.

02

Audio lockdown with kids

Their TikTok and Instagram audio is training data. Set accounts to private. Disable comments on minors' posts. Audit who's in their followers list every quarter — most of them are bots.

03

Shared password manager · family vault

1Password Families or Bitwarden Family. Shared vault for streaming services, Wi-Fi, common accounts. Personal vault per person — sacred. Teaches kids password hygiene by osmosis.

04

Travel protocol

Before anyone in the family travels: location-sharing on for the trip only, public posts off until home, hotel Wi-Fi only with VPN, no banking from public networks. Default state, every trip.

CHAPTER 06 · FAMILY OPSEC

The household quarterly · 30 minutes, 4× a year

- [ ] Review password manager — any reused passwords flagged? Replace.
- [ ] Check haveibeenpwned for every household email.
- [ ] Revoke app permissions you haven't used in 90 days.
- [ ] Update OS on every device — phone, laptop, router, smart TV.
- [ ] Re-test the family memory key. Without warning. Once.

> Your perimeter is everyone you love. Harden the people, not just the devices. The devices change every two years. The people don't.

EMERGENCY CARD · CUT & CARRY

IF SOMETHING JUST WENT WRONG

READ TOP TO BOTTOM. DON'T SKIP.

01 Disconnect the device. Airplane mode. Wi-Fi off.

02 Move to a different device on a different network.

03 Change passwords: email → bank → social.

04 Force log-out of all sessions.

05 Freeze credit reports.

06 Notify bank via app or branch — never call back.

07 Document everything. Screenshots. Times.

08 File police report if monetary loss.

09 Do not click "recovery" links sent after the fact.

10 Wait 24 hours before public posts. They watch.

WHERE I LEAVE YOU

This is the floor. Not the ceiling.

The full Field Manual is over a hundred pages. Quarterly updates. A live threat library. Decryption guides for the breaches you're already in. Templates for every conversation in this booklet.

FIELD MANUAL · FULL	100+ pages · quarterly updates · threat library	snayr.dev/manual
SENTINEL CIRCLE	Weekly threat brief · private community · live AMAs	snayr.dev/circle

Send this manual to one person tonight. That's the deal.

Stay sharp.

SNAYR · snayr.dev