

Answer Key — Persona Audit

Admin / self-check reference

Compare each finding against your own list. The point is not to get exactly seven matches; the point is to notice that every line of the profile contains a separate contamination vector. A persona is the union of all of them, not any single one.

Finding 1 — Shared device

Finding: The persona runs on the same MacBook the operator uses personally.

Why it breaks the persona: Device fingerprints (fonts, GPU, canvas, audio context, WebGL renderer, installed software, client build numbers) are stable across personas on the same machine. Any provider that sees both accounts will get an identical device fingerprint. Telemetry from background tools — auto-updaters, crash reporters, IDE analytics — carries a persistent installation ID that ties every account on the machine together.

Remediation: Use a dedicated VM or, better, a separate physical device. The VM must be provisioned fresh and must never share a clipboard, filesystem, or network namespace with the host's personal state.

Finding 2 — Default browser profile with real-identity logins

Finding: Chrome's default profile already contains 12 real-identity logins.

Why it breaks the persona: A browser profile is a shared context. Cookies, localStorage, service workers, extensions, and site data from the 12 real-identity sessions are accessible to every tab in the profile. Third-party scripts that recognize any one of those logins can correlate the persona session to the real identity in real time, and cross-site recommendation systems will link them through simple co-occurrence.

Remediation: A fresh, empty browser profile dedicated to this persona and nothing else. No extensions, no sync, no saved logins from any other account. If more than one

persona exists, each one gets its own profile — no exceptions.

Finding 3 — Personal credit card on the persona account

Finding: The persona ProtonMail account is paid for with the operator's personal credit card.

Why it breaks the persona: The billing database permanently links the persona account to the operator's real billing name, address, and card BIN. That link is durable, provider-attested, and subpoenaable. Any future investigator can pivot from the persona to the real identity in a single query against the provider's payments system. No amount of device, network, or stylometric discipline saves a persona whose billing record points to the operator.

Remediation: Fresh payment trail. A prepaid card bought for cash, a virtual card issued under a different identity, or another funding source that shares no billing name, address, or BIN country with the operator's real cards.

Finding 4 — OAuth via the operator's real Google account

Finding: The "burner-dev-42" GitHub account was created with "Log in with Google" against the operator's real Google identity.

Why it breaks the persona: OAuth is a correlation primitive. Google now has a provider-attested record that "burner-dev-42" and the operator's real Google identity are the same person, and so does GitHub. Unlinking the OAuth grant later does not delete the server-side attestation. The persona GitHub account is linked to the real identity forever, by both providers, with cryptographic evidence.

Remediation: Burn the GitHub account. Create a new one using email and password only, from the persona device, on the persona network, with the persona's dedicated email address. Never click "Log in with X" on any persona account, for any reason, ever.

Finding 5 — Distinctive catchphrase leaks across accounts

Finding: Four persona prompts end in "let's ship it" — a phrase the operator uses in real-life Slack every day.

Why it breaks the persona: This is a stylometric beacon. A distinctive idiom that appears on both sides of a persona boundary is exactly the signal a content-analysis pipeline is designed to catch. Stylometric classifiers do not need many examples to link

accounts — a handful of occurrences of a rare phrase is enough, and "let's ship it" is rare enough to be high-signal.

Remediation: Write the persona a different vocabulary, deliberately chosen. Maintain a voice document for the persona — opening phrase, closing phrase, preferred idioms, punctuation style — and re-read it before every session. The operator's natural idioms do not appear anywhere in the persona's output. Ever.

Finding 6 — Matching timezone

Finding: The persona device is configured to the operator's home timezone.

Why it breaks the persona: Timezone is both a device fingerprint field (reported by the browser via the JS timezone API) and a behavioral signal (the persona is active during the operator's normal hours). Matching timezone narrows the candidate population dramatically and is one of the easiest bits to correlate across accounts because it is stable and cheap to measure.

Remediation: Drift the persona's timezone to something consistent with the persona's cover story — or, at minimum, never let the persona's messages reference local time, day of week, or "it's late here" style hints. Behavioral timing should be deliberately scheduled, not driven by the operator's natural rhythm.

Finding 7 — Personal extensions in the persona browser

Finding: Grammarly is installed and signed into the operator's personal Grammarly account; 1Password is signed into the operator's personal vault.

Why it breaks the persona: Grammarly sees every keystroke on every page where the extension is active — including every persona prompt — and uploads telemetry tied to the operator's personal Grammarly account. 1Password's personal vault logs every autofill against the operator's personal 1Password identity. Both of these silently link every persona action to the operator in the respective vendor's systems. Neither of them is visible in the AI provider's dashboard, which is exactly why they are dangerous.

Remediation: Remove personal-account extensions from the persona browser profile entirely. If a password manager is needed, use a separate vault that contains only persona credentials. If grammar assistance is needed, use an offline tool. Default

posture: the persona profile has no extensions at all unless each one has been explicitly justified.