

DAXXIS

A DAXXIS FIELD GUIDE

The 3-Tier Vault



A Practical Security Architecture for
Solo Founders and Small Firms

Build it in an afternoon. Run it in minutes a week. Memorize exactly
three things.

Three in your head, everything else in the system.

Optimization with Optimism

Could you tell someone your bank password right now?

If you can, that is the problem this guide fixes. For most one-person businesses, security looks like passwords saved in a browser, sensitive files in folders named “Important” and “Important_FINAL,” and two-factor codes going to a phone you could drop in a parking lot tomorrow. One phished email, one stolen laptop, one bad afternoon — and you are locked out of your own business, or someone else is in it.

The fix is not one magic tool. It is three plain tools, each doing one job, arranged so no single failure takes you down:

- **Tier 1 — The Credential Vault.** A password manager (Bitwarden) holds every login. It remembers hundreds so you don't have to.
- **Tier 2 — The File Vault.** An encrypted container (VeraCrypt) holds the documents that would actually hurt you if they leaked.
- **Tier 3 — The Identity Root.** A hardware security key plus disciplined two-factor setup makes your most important accounts un-phishable — with paper recovery codes, so you can never be locked out of your own life.

Cost: Bitwarden's free tier and VeraCrypt (free, open source) cover Tiers 1 and 2 entirely. The only money in this build is the hardware key (\$25–60). And if money is tight this month, there is a free way to start: section 3.5 (page 9) shows how to get most of the protection at \$0 and add the key later.

After build day, the whole system runs on about five minutes a week — daily is nothing, and that is the design. The Rhythm (page 10) is the entire maintenance plan.

First move

Print the worksheets — pages 11–13 (jump there). You will fill them in as you build, and every worksheet this guide mentions lives there.

Read this before you build anything

Here is the single organizing idea that makes this whole system manageable. When you are done building, you will memorize exactly three secrets. Three. Not thirty.

- **1. Your device login** — the passphrase that unlocks your computer.
- **2. Your Bitwarden master passphrase** — the one that unlocks every stored credential.
- **3. Your VeraCrypt container passphrase** — the one that unlocks your sensitive files.

Everything else in your life gets one of two treatments: **STORED** (a long random password that lives in Bitwarden — you will never read it, type it, or remember it) or **REGISTERED** (protected by your hardware key or an authenticator app, tracked on a one-page registry).

That is the org chart: three in your head, everything else in the system. Worksheet 1 (page 11) is the physical page for The Three. Fill it in as you build, in pen, and it becomes the heart of your Emergency Sheet. The Three live in two places only: your memory and that sealed sheet. Never in a file, a photo, a note app, or an email draft. Paper cannot be phished.

Make each of The Three a different four-word passphrase. The method, concretely:

- Aim for something like: **Granite-Pelican-Voltage-Hymn** — four unrelated words, joined with dashes, one capital letter.
- Two easy ways to pick your four words: open any paperback to four random pages and take the first noun your finger lands on — or use the EFF wordlist, a free list of everyday words built for exactly this (search “EFF large wordlist”) and roll dice to pick.
- Test: 20+ characters, no names, no dates, no addresses, nothing a person who knows you could guess. Random is the entire point.
- If your computer currently unlocks with a short PIN or no password: fix that now (Windows: Settings → Accounts → Sign-in options; Mac: System Settings → Users & Groups). Your device login is one of The Three — treat it like one.

■ **Done looks like:** Worksheet 1 has three distinct passphrases written in pen, none reused anywhere, and your computer no longer opens with 1234.

TIER 1: The Credential Vault (Bitwarden)

Time: 60–90 minutes. Cost: \$0.

1.1 Create the account

- Go to bitwarden.com → Create account.
- Email: your business email — this account is business infrastructure.
- Master password: The Three #2 from Worksheet 1 (page 11). Type it from the paper — that is your first retrieval drill.
- Skip the password hint. A hint that helps you helps a stranger.

1.2 Install in three places

- **Desktop app** — bitwarden.com/download.
- **Browser extension** — same page; install it in the browser you actually work in. After installing, click the puzzle-piece/extensions icon and pin the Bitwarden shield to the toolbar so it is always visible.
- **Phone app** — App Store / Play Store. Sign in on all three.

1.3 Move your logins in — then burn the bridge

- **Export from your browser.** Every major browser has this; the wording shifts between versions, so use the search box inside Settings — type “export” and you will land on Export passwords (Chrome/Edge/Brave keep it under the password-manager or autofill section). It produces a CSV file.
- **Import to Bitwarden:** sign in at the website vault → Tools → Import data → set the format to your browser's CSV (e.g., “Chrome (csv)”) → choose the file → Import.
- **Burn the bridge — this is not optional:** delete the CSV (it is your entire digital life in plaintext); empty the Recycle Bin / Trash; check Downloads for a second copy; delete that too.
- **Turn the browser's own password manager OFF** (Settings → search “passwords” → toggle off Offer to save passwords) and delete everything it stored (same screen). If your passwords live in two places, you can never be sure which copy is right. One vault. One truth.

■ **Done looks like:** the Bitwarden extension shows your login count; your browser's password list shows zero; visiting one of your sites and clicking the Bitwarden shield offers the right login.

1.4 Re-key the five accounts that matter most (just five today — not all of them)

Today you fix five passwords. The rest you fix whenever you next touch them. The five:

- **1. Business email** — it can reset everything else, so it goes first
- **2. Personal email** — it can reset half your life
- **3. Bank / financial institution**
- **4. Phone carrier** — a stolen number intercepts text codes

- **5. Payment processor** — anything that moves business money

For each: log in → account/security settings → change password → in the Bitwarden popup click the generator (the circular-arrows icon) → set length 20+, all character types → save the generated password into Bitwarden when prompted. You never see, read, or remember these. That is the system working.

Log each one on Worksheet 2 (page 12) as you go — checkbox, not password. Worksheets hold inventory, never secrets.

■ **Done looks like:** five rows checked on Worksheet 2; logging into your bank requires a Bitwarden autofill because you genuinely do not know the password anymore. That feeling of “I couldn't tell you my own bank password” is correct — it is the point of the whole tier.

1.5 The Emergency Sheet (start it now, finish it in Part 3)

Worksheet 4 (page 13) is the template. Fill in now: The Three, your Bitwarden account email, today's date. It gets sealed after Part 3 adds recovery codes. Destination: a fire safe, a bank box, or a trusted relative — wherever your passport-grade things live.

