Create a Club Continuity Vault
(from AI by Allan Milbradt)

Why?
Most club nowadays have a website, a Facebook page and other online accounts. Usually, one person is in charge of these accounts and knows the passwords and other passkeys or access is linked to a cell phone. What happens when that person is no longer available? All access are lost.

What?
Here are some ideas on how to Create a Club Continuity Vault How would this work? Most accounts now for everything have two step verification. How would you ever allow access to this so you wouldn't lose contact to these accounts?

How?
The issue is that most accounts access require a password AND Two-factor authentication (2FA). They are designed to stop exactly this kind of "shared access," which makes it tricky for legitimate succession planning. Here's how it actually works in practice.

- **The Core Tool: A Shared Password Manager**

The foundation is an organizational password manager — Bitwarden (free tier works fine for small clubs) or 1Password (paid, but has a "Families" or "Teams" plan). These aren't just password storage; they can also generate 2FA codes on behalf of multiple people. That's the key feature that solves your problem.

- **Solving the 2FA Problem**

There are three types of 2FA, and each has a different fix:

  - **App-based codes (Google Authenticator, Authy style)** When you set up this kind of 2FA, the service shows you a QR code and a "secret key" string. Most people scan it once and forget it — but that secret key can be saved as text in the password manager entry. Modern password managers (Bitwarden, 1Password) can store that secret and generate the same rotating codes themselves. So instead of one person's phone being the only source of the code, *anyone with vault access* can open the password manager and get the current code.
  - **Backup codes** When 2FA is enabled, almost every service generates a set of 8–10 one-time-use backup codes "in case you lose your device." Most people never look at these again. Save them as a note in the vault entry. If something goes wrong, an officer can use one of these to log in and reset 2FA entirely.

    - **SMS-based codes** This is the riskiest type, because it's tied to a personal phone number — if that person disappears, so does the phone. The fix: get a club-owned phone number through Google Voice (free) and use that number for any account that insists on SMS 2FA. Google Voice can forward texts to email, which multiple officers can access.
    -

- **Prefer "Multi-Admin" Over "Shared Login" Where Possible**

For some platforms, the better answer isn't sharing one login at all — it's using the platform's built-in multi-user features, which sidesteps the 2FA problem entirely:

- **Facebook/Instagram** — convert the page to a Business/Page with multiple Admins. Each officer logs in with their *own* account and their *own* 2FA. No shared credentials needed.
- **Google Workspace** (if the club upgrades from a personal Gmail to a Workspace account) — multiple users, each with admin rights, each with their own 2FA.
- **Mailchimp/newsletter tools** — most support multiple team members natively.

This is actually the gold-standard fix: nobody is sharing secrets, and there's no single point of failure to begin with.

- **Where Shared Login Is Unavoidable**

Some things genuinely have one login — domain registrars (GoDaddy, Namecheap), some bank portals, a personal Gmail being used as the "club email." For these:

- Use the password manager's TOTP storage as described above
- Set the account's recovery email to a club-controlled address (not a personal one)
- Store the backup codes in the vault

Who?

Governance — Who Holds the Keys

- **3–4 officers** get accounts in the shared vault (most password managers let you grant access without revealing the actual master password)
- **The vault itself is protected by a master password** that's written down once, sealed in an envelope, and given to a trusted person outside the immediate officer group — like a long-time member or a neighboring club's president
- **Annual review**: at the same time as elections, do a 15-minute "vault check" — confirm logins still work, remove departed officers, add new ones

When? Now ! Practical First Step

Set up Bitwarden's free organization plan, have the current club leader go through every account (email, Facebook, domain, bank, newsletter), and for each one: save the password, save the 2FA secret/backup codes, and where possible add a second admin directly on the platform. This is a few hours of work that would save a club from disappearing.