Two-factor codes that don't leave with the person

Almost every church has its two-factor codes going to one person's phone, because that's who set the account up. It works perfectly until they leave, and then the church cannot get into its own email, its own Facebook page, or its own giving platform — and the person who *could* help is a former employee, or has moved 300 miles, or is the pastor you just said goodbye to. This page is how to fix that when the church owns no phones and has no IT budget, which describes most of us.

Before you start

The rule you're aiming for, in one sentence: the second factor should live somewhere the *church* keeps, not somewhere a *person* keeps.

What you need first. A list of the accounts that matter — see gathering your records if you don't have one yet. You cannot fix what you can't enumerate.

What this will cost. Between nothing and about $50 a year for most churches. The expensive part is attention, not money.

Who owns it. One named person — usually the office administrator or the pastor — with a second person who knows where everything is kept. Never one person alone; that's the problem you're solving.

A word about panic. You do not have to fix every account this week. Fix church email first, because it's the recovery address for everything else, and work down from there.

The workflow

Phase 1 — Pick the church's method

Choose one of these as your default. Most churches land on the first.

A shared password manager with built-in authenticator. The church's vault holds both the password and the two-factor code generator, in a shared folder that two or three officers can open. Anyone authorized can get in; nobody personally owns it. Bitwarden and 1Password both do this, both have free or low-cost tiers, and both are cheaper than one lockout.

- *Cost:* free to about $4/month.
- *Strength:* solves passwords and two-factor at once, and it's the same place your Itineracy vault pointers will point to.
- *Watch out for:* the master password becoming a one-person secret. Two people know it, and it's written down in the safe.

A cheap device that stays in the office. An old smartphone or a $30 tablet, kept in a locked drawer, on wifi, running an authenticator app. No cell plan needed if you avoid SMS codes.

- *Cost:* one-off, often nothing if someone donates an old phone.
- *Strength:* physical, obvious, hard to misunderstand.

- *Watch out for:* the battery dying and the device being forgotten. Charge it monthly; note it on the maintenance schedule.

A church-owned phone number. A free Google Voice number, or a cheap VoIP line, that forwards to whoever is on duty and can receive SMS codes.

- *Cost:* free to a few dollars a month.
- *Strength:* works for accounts that only offer SMS.
- *Watch out for:* SMS is the weakest form of two-factor, and Google Voice can't be the second factor for the Google account it belongs to.

Hardware keys. Two YubiKeys — one in the safe, one with the office. Best security available.

- *Cost:* roughly $30–60 each, and buy two.
- *Strength:* essentially unphishable.
- *Watch out for:* losing both. The backup codes matter more here than anywhere.

Phase 2 — Fix church email first

- ☐ Turn on two-factor for the church's email/Google Workspace account, with the second factor pointed at the method you chose.
- ☐ Set the **recovery address** to a role address the church controls (`office@`), not a personal one.
- ☐ Print the **backup codes** and put them in the church safe. Write the date on them.
- ☐ Record in the account register where the codes are and where the vault is.

Do this one first and stop for the day if you need to. Church email is the recovery path for nearly every other account; securing it makes everything else recoverable.

Phase 3 — Work down the list

For each remaining account, in this order — money, then presence, then the rest:

- ☐ Bank, giving platform, payroll.
- ☐ Facebook page, website host, domain registrar.
- ☐ Everything else.

For each one:

- ☐ Turn on two-factor if it's off.
- ☐ Point the second factor at the church-held method.
- ☐ Save backup/recovery codes to the safe.
- ☐ Record the destination in the register — the actual destination, in words a stranger would understand.
- ☐ Remove personal devices that no longer need to be there.

Phase 4 — Make it survive

- ☐ Two people know how to open the vault or unlock the device.
- ☐ Backup codes are in the safe, dated, and listed in the document register.
- ☐ The register says where everything lives.

- ☐ Put a recurring annual check in the church calendar — the same month every year — to confirm the destinations still work and the leavers are gone.

Who does what

Task	Owner
Choosing the method	Pastor with the office administrator; tell the trustees
Paying for it	Finance committee — it's a line item, and a small one
Doing the migration	One named person, with a second who knows where things are
Holding the backup codes	The church safe; trustees know it exists
Annual check	Whoever keeps the account register

Variations

A church with no office and no safe. A locked filing cabinet at the church, or a sealed envelope with the treasurer, both work. What doesn't work is "in my desk at home."

A one-person office. This is the hardest case and the most important. The second person doesn't have to be staff — a trusted lay leader, the SPRC chair, or a trustee can hold the second copy. The point is that no single departure loses the church its accounts.

A church mid-pastoral-transition. Do this *before* moving day, not after. An outgoing pastor is glad to help in May and hard to reach in August. If it's already August, ask anyway — most people are willing, they're just busy.

A church where the accounts are on a volunteer's personal setup. Extremely common with websites and social media. Have the conversation early and without accusation: it isn't distrust, it's what happens when they move, get ill, or step back. Ask them to create a church-owned account and transfer ownership, and thank them properly — they were solving a problem nobody else would.

Accounts that offer no two-factor at all. Some smaller vendors don't. Record that fact rather than leaving it blank, use a unique password from the vault, and note it as a known risk.

Elsewhere

- **More than a Password — CISA** — the U.S. cybersecurity agency's plain-language case for multi-factor authentication, useful if you need to persuade a committee.
- **Turn on 2-Step Verification — Google** — the actual steps for the account most churches should fix first.
- **Bitwarden for business** — shared vaults with a built-in authenticator; the free tier covers a small church.
- **1Password for business** and **using 1Password as an authenticator** — the same approach; ask about nonprofit pricing.
- **Google Voice** — a free church-owned number for accounts that only send SMS codes.
- **YubiKey Security Key series** — hardware keys, if you want the strongest option. Buy two.
- **Key log** — the physical-access twin of this page. Same principle: record who holds what, never the code itself.

This is a starting point, not legal advice. Employment law varies by state, and your annual conference may have policies that go beyond the Discipline. Before you rely on anything here for a hiring, firing, or compensation decision, run it past your conference office or chancellor.