Small Organization Digital Security Starter Kit

Introduction: Security Is Continuity

Small organizations rarely have a dedicated IT department. Access gets shared informally. Volunteers rotate in and out. Tools get layered over time.

Most security failures in small teams are not caused by sophisticated attackers. They are caused by shared passwords in documents, domains registered under personal accounts, or no one knowing who controls hosting.

Security is not about becoming unhackable. It is about ensuring your organization can continue operating when something goes wrong.

Step 1: Control Access Before Anything Else

Separate personal and organizational accounts

A common mistake is using personal email accounts to manage domains, hosting, payment processors, or social media platforms.

This creates risk because password resets go to personal inboxes, access leaves when a volunteer leaves, and compromised personal accounts can expose your entire organization.

Instead, create role-based email accounts tied to your domain:

- admin@yourorg.org
- info@yourorg.org
- treasurer@yourorg.org
- webmaster@yourorg.org

Use these accounts to register domains and critical services. Forward them to relevant team members, but ensure the credentials are stored in a shared password manager.

Stop sharing passwords in documents or chat

Sharing passwords in Google Docs, Slack messages, email threads, or text messages permanently reduces your control over them.

Messages can be forwarded. Documents can be copied. Former members may still have access. You cannot easily rotate credentials everywhere they were shared.

A better alternative is to use a shared password manager such as:

- Bitwarden (Teams)

- 1Password Teams
- Proton Pass for Business

Generate unique passwords (20+ characters), store them in shared vaults, and remove members immediately when they leave.

Enable multi-factor authentication everywhere

Passwords alone are not sufficient. Breaches, phishing, and credential stuffing attacks are common and automated.

Enable multi-factor authentication on:

- Email accounts
- Domain registrar
- Hosting provider
- Cloud storage
- Payment processors
- Messaging platforms

Prefer authenticator apps or hardware security keys over SMS, which is more vulnerable to SIM-swapping attacks.

Create a documented offboarding checklist

When someone leaves an organization, access is often forgotten. Over time, inactive accounts accumulate and create risk.

Create a standard checklist:

- Remove them from the password manager
- Disable or remove email access
- Remove hosting and domain dashboard access
- Remove payment processor access
- Remove shared drive and messaging platform access
- Rotate shared passwords if necessary

Offboarding should be procedural, not memory-based.

Step 2: Domain and Website Control

Know who owns the domain

If a volunteer registers your domain under their personal account, renewal notices and recovery emails go to them.

If their card expires or they leave the organization, your domain can lapse. Domain expiration can lead to downtime, email failure, and reputational damage.

Instead:

- Register domains using an organizational role email
- Enable auto-renew
- Ensure at least two trusted members have access
- Store registrar credentials in your password manager

Document hosting and backups

Many small organizations cannot clearly answer: Where is the site hosted? Who can log in? Are backups automated?

Without clear answers, recovery becomes slow or impossible during an incident.

At minimum, document:

- Hosting provider
- Account login location
- Backup frequency
- Backup storage location

Enable automated backups and periodically test restoring them. A backup that has never been tested is only a theory.

Reduce plugin and integration sprawl

Adding new plugins or integrations for every feature request increases maintenance burden and attack surface.

Abandoned plugins or poorly maintained integrations become long-term security liabilities.

Before adding a tool, ask:

- Can we accomplish this with existing tools?
- Is this actively maintained?
- Does it require admin-level permissions?

Simpler systems are easier to secure and easier to maintain.

Step 3: Communication and Messaging Hygiene

Limit administrative roles

Many teams grant admin privileges to anyone who “needs access.” Over time, this leads to too many people having high-level control.

Administrative access allows users to:

- Add or remove members
- Export data

- Change security settings
- Delete content or entire workspaces

The more admins you have, the larger your risk surface becomes.

Instead, apply the principle of least privilege:

- Only assign admin roles to those who truly need them
- Review admin lists quarterly
- Require MFA for all admin accounts

Avoid tying messaging platforms to personal ownership

It is common for Slack, Discord, or similar workspaces to be created under a founder’s personal email account.

This becomes risky if that person leaves or loses access. Platform ownership should belong to the organization.

Instead:

- Transfer workspace ownership to a role-based organizational account
- Ensure at least two trusted members have owner-level access
- Store recovery codes securely in your password manager

Email and shared inbox practices

Forwarding everything to personal inboxes can blur boundaries and complicate access management.

A more secure alternative is:

- Use shared inbox tools or group mailboxes
- Maintain role-based accounts for external-facing communication
- Disable automatic forwarding when someone leaves

Clear ownership prevents confusion during transitions.

Step 4: Data Awareness and Minimization

Know what data you collect

Many small organizations collect more data than they realize: email lists, donor records, volunteer spreadsheets, form submissions, or even copies of identification documents.

Every piece of stored data increases your responsibility. If it is exposed, your organization bears the consequences.

Start by listing:

- What data you collect
- Where it is stored

- Who has access
- How long it is retained

Collect only what you truly need

If you do not need certain information to operate, do not collect it.

Data you never collect cannot be breached.

Review forms and systems regularly and remove unnecessary fields.

Secure payment processors

Platforms like Stripe or PayPal often hold sensitive financial information. Compromise here can have immediate consequences.

Avoid:

- Sharing payment logins casually
- Leaving former volunteers with financial access
- Using weak or reused passwords

Instead:

- Enable MFA on all payment accounts
- Restrict admin-level access to essential personnel
- Review access quarterly

Step 5: Prepare for Incidents Before They Happen

Create a simple phishing response rule

Phishing attempts are one of the most common threats small organizations face.

Implement a “pause rule”:

- No urgent financial actions without secondary verification
- Verify unusual requests via a second channel
- Do not share verification codes or MFA tokens with anyone

Have a basic response plan

If you suspect an account compromise:

- Disconnect the affected account if possible
- Change passwords immediately
- Rotate shared credentials
- Revoke active sessions and API keys
- Inform relevant team members

Document these steps in advance so you are not improvising under stress.

Minimum Viable Security Checklist

If you only implement a small number of changes, start here:

1. Use role-based organizational email accounts
2. Adopt a shared password manager
3. Enable multi-factor authentication everywhere
4. Enable domain auto-renew and document registrar access
5. Ensure at least two trusted members can access critical systems
6. Automate website backups
7. Limit admin privileges across platforms
8. Create and follow an offboarding checklist
9. Audit payment processor access
10. Document a simple incident response plan

Sustainable systems are more important than sophisticated ones. Simplicity reduces both burnout and risk.