DESKREADY

FREE RESOURCE · CHECKLIST

The small-org security checklist

Six areas, plain language, no jargon. Work down the list. None of this is hard, and each one closes a door that attackers and data brokers count on being left open.

1 Passwords

- Use a password manager (Proton Pass, Bitwarden, 1Password, or KeePass) so every login can be different.
- Make every account a unique password, never reused, not just the important ones.
- Change any password you've used in more than one place, starting with email.

2 Two-factor authentication (2FA)

- Turn on 2FA for email first, it's the master key that resets everything else.
- Add 2FA to your domain registrar, banking, and any money or customer systems.
- Prefer an authenticator app or a hardware key over text-message codes.

3 Backups you control

- Keep your own copy of anything you can't afford to lose, not just the vendor's.
- Follow 3-2-1: three copies, two types of storage, one off-site.
- Actually test a restore, a backup you've never opened isn't a backup yet.

4 Own your domain

- Make sure the domain is registered in your organization's own registrar account.
- Use an email address you control as the owner contact, not a vendor's or a former employee's.
- Turn on auto-renew plus a backup payment method so it can't lapse.

5 Keep things updated

- Turn on automatic updates for your devices, browsers, and key software.
- Replace anything that no longer gets security updates.
- On your website, keep the platform and plugins current (or have someone do it).

6 Remove access when people leave

- Keep a short list of who has access to what (logins, shared accounts, keys).
- Revoke access the day someone leaves, including any shared passwords they knew.
- Review the list a couple of times a year and close anything unused.

Want a hand with any of these? We'll audit your setup and fix the gaps with you, or for you. **Book a free consult →**

412-353-9161 · **deskready.com**