Intrada TECHNOLOGIES

# BUILD A PASSWORD THAT WORKS




Your password is the lock on your digital front door. A weak one invites trouble — a strong one buys you time and protection.

## Recommended Strong Password Specifications

- **Minimum 12-14 characters** (longer beats more complex)
- At least **One Uppercase Letter**
- At least **One Number**
- At least **One Symbol** (!, @, #, $, etc.)
- Use the **Keyboard-Shift Method** to turn a memorable phrase into a strong password:
  Phrase: "MyHairyDogDug"
  Shift each key up & to the left: **J6Yq846E9tE7r**
- **Unique Password for Every Account** – vary it by service (e.g., "MyHairyBankDug" for your bank login)
- Use a **Password Manager** (Keeper, LastPass, 1Password, or Bitwarden) to store and generate passwords
- **Enable Multi-Factor Authentication (MFA)** on every account that offers it – email, banking, and social media included

## Things to AVOID

- Reusing the same password across multiple accounts
- Sharing passwords with coworkers, friends, or family
- Using common words, names, or simple number sequences ("password123," "qwerty")
- Using personal information that's easy to find (birthdays, pet names, addresses)
- Writing passwords on sticky notes or unsecured documents
- Skipping MFA when it's available
- Using the same password for years without updating it
- Trusting "strong-looking" passwords without checking if they've been part of a data breach

Questions about your security setup? **Contact us** for a review, training, or help building stronger password policies across your organization.

Intrada Technologies™ 2026 – All rights reserved.

31 Ashler Manor Drive
Muncy, PA 17756

**intradatech.com**
570-321-7370

Exceeding Expectations.