

Password Management Made Simple

A Friendly Guide to Keeping Your Accounts Safe

Passwords protect everything important online — your email, your banking, your photos, and your personal information. This guide will show you how to create strong passwords, manage them easily, and keep your digital life secure.

Did You Know?

- The average person has 100+ online accounts
- 81% of data breaches are caused by weak or stolen passwords
- A 12-character password takes 62 trillion times longer to crack than a 6-character one
- Using a password manager reduces your risk of being hacked by up to 80%

What Makes a Password Secure?

Not all passwords are created equal. Here's what separates a strong password from a weak one:

1. Length is King

The longer your password, the harder it is to crack. Every additional character makes it exponentially more difficult for hackers to guess.

- 6 characters: Cracked instantly
- 8 characters: Cracked in hours
- 10 characters: Cracked in weeks
- 12 characters: Cracked in years
- 16+ characters: Virtually uncrackable

Our Recommendation: Use at least 12 characters, ideally 16 or more.

2. Mix It Up (But Don't Stress)

A good password includes a variety of character types:

- Uppercase letters — A, B, C...
- Lowercase letters — a, b, c...
- Numbers — 0, 1, 2, 3...
- Special characters — !, @, #, \$, %, &...

Pro Tip #1: Length matters more than complexity. A long, simple password is often stronger than a short, complex one.

3. Avoid Predictable Patterns

Hackers use software that tries common patterns first. Avoid:

- X Personal information (birthdays, pet names, addresses)
- X Common words (password, qwerty, letmein)
- X Simple patterns (123456, abcdef, 111111)
- X Keyboard patterns (qwerty, asdfgh)
- X Single words from the dictionary
- X Your username, email, or name of the organization associated with the account

4. One Password Per Account

This is crucial: Never reuse passwords across different accounts. If one account gets hacked, all your other accounts remain safe.

Warning: When a company has a data breach, hackers try those stolen passwords on other popular sites. If you reuse passwords, one breach can compromise everything.

How to Create Strong Passwords

Method 1: The Passphrase (Recommended for Memorable Passwords)

A passphrase is a series of random words strung together. It's long, strong, and surprisingly easy to remember.

How to create one:

1. Pick 4-5 completely random, unrelated words
2. Connect them with dashes, numbers, or symbols
3. Add a capital letter and number

Examples:

```
purple-Elephant-dances-42-slowly  
correct-horse-Battery-staple  
Mango!bicycle*sunset2piano  
ocean-Trumpet-7-blanket-coffee
```

Pro Tip #2: Why this works: "purple-Elephant-dances-42-slowly" is 32 characters long and would take millions of years to crack, but it creates a silly mental image that's easy to remember!

Method 2: Let a Password Manager Create It (Best Option)

Password managers can generate truly random passwords like:

x7#Km9\$pL2@qR5nW or Bf4!hNc8#Yw2\$Zp6

You don't need to remember these — the password manager does it for you! More on password managers in the next section.

What NOT to Do

- X password123 — Too common and predictable
- X John1985 — Contains personal info (name + birth year)
- X qwerty!@# — Keyboard pattern + common symbols
- X Summer2024! — Seasonal pattern hackers know to try
- X IloveMyDog — Common phrase structure

Password Managers: Your Digital Keychain

A password manager is a secure app that stores all your passwords in one place. You only need to remember one master password — the manager remembers everything else.

Why Use a Password Manager?

- ✓ **Remember just one password** — Your master password unlocks everything
- ✓ **Generate strong passwords** — Creates random, uncrackable passwords for you
- ✓ **Auto-fill login forms** — No more typing! Passwords fill in automatically
- ✓ **Sync across devices** — Access your passwords on phone, tablet, and computer
- ✓ **Spot fake websites** — Won't auto-fill on phishing sites that look real but aren't
- ✓ **Secure notes** — Store other sensitive info like PINs and security questions

Option 1: Built-In Password Managers (Free & Easy)

If you're new to password managers, start with the one already on your device:

Apple Passwords (iPhone, iPad, Mac)

Built right into your Apple devices. Syncs automatically via iCloud. Find it in Settings [®] Passwords.

Pros: Free, seamless on Apple devices, suggests strong passwords, warns about breaches

Cons: Only works well within Apple's ecosystem

Google Password Manager (Chrome, Android)

Built into Chrome browser and Android phones. Syncs with your Google account. Find it at passwords.google.com.

Pros: Free, works anywhere Chrome works, password checkup feature

Cons: Tied to Google account, less robust than dedicated managers

Microsoft Authenticator (Windows, Edge)

Built into Microsoft Edge and Windows. Syncs with your Microsoft account.

Pros: Free, integrates with Windows, includes 2FA features

Cons: Best experience limited to Microsoft ecosystem

Pro Tip #3: These built-in options are a great starting point and far better than reusing passwords or writing them on sticky notes!

Option 2: Dedicated Password Managers (More Features)

For more security features and cross-platform flexibility, consider a dedicated password manager:

OUR TOP RECOMMENDATION: Proton Pass

Proton Pass is made by Proton, a Swiss company dedicated entirely to privacy and security. They also make ProtonMail (secure email) and ProtonVPN.

- ✓ **End-to-end encryption** — Even Proton can't see your passwords
- ✓ **Swiss privacy laws** — Some of the strongest data protection in the world
- ✓ **Open source** — Security experts can verify the code
- ✓ **Free tier available** — Unlimited passwords, unlimited devices
- ✓ **Works everywhere** — iOS, Android, Chrome, Firefox, Safari, Edge
- ✓ **Email aliases** — Hide your real email when signing up for online accounts
- ✓ **Secure notes** — Store sensitive information safely, such as credit card details

Website: <https://proton.me/pass>

Cost: Free tier available; Premium ~\$4/month

Other Reputable Options:

- 1Password (\$3-5/month)
Excellent family sharing, travel mode, polished apps
- Bitwarden (Free / \$10/year)
Open source, very affordable, self-host option
- Dashlane (\$5-7/month)
Built-in VPN, dark web monitoring, easy to use

Note: We recommend avoiding LastPass due to past security breaches. While they've improved, alternatives like Proton Pass offer better security track records.

Getting Started with a Password Manager

Ready to upgrade your password security? Here's how to get started:

Step 1: Choose your password manager

Start with your device's built-in option (Apple Passwords, Google Password Manager) or try Proton Pass for more features and increased privacy regulations.

Step 2: Create a strong master password

This is the ONE password you need to remember. Make it a long passphrase like "In2022IwenttoMexico!" that you won't forget.

Step 3: Install on all your devices

Get the app on your phone, tablet, and computer so your passwords sync everywhere.

Step 4: Start with your most important accounts

Update passwords for email, banking, and shopping sites first. Let the password manager generate a new, strong password that you can update for each online account.

Step 5: Gradually add other accounts

Each time you log into a site, save the password to your manager. Over time, you'll have everything stored securely.

Step 6: Enable two-factor authentication (2FA)

For extra security on important accounts, enable 2FA. Many password managers can store these codes too.

Pro Tip #4: Don't try to do everything at once! Start with 5-10 important accounts, such as your banking. Add more accounts over the coming weeks as you naturally log into different sites.

Quick Reference: Password Do's and Don'ts

DO:

- ✓ Use 12+ characters (16+ is even better)
- ✓ Use a unique password for every account
- ✓ Use a password manager to generate and store passwords
- ✓ Enable two-factor authentication on accounts
- ✓ Update passwords immediately when a service provider announces a breach
- ✓ Use passphrases for passwords you must remember

DON'T:

- ✗ Reuse passwords across multiple sites
- ✗ Use personal information (birthdays, names, addresses)

- X Share passwords via email or text message
- X Write passwords on sticky notes stored near your computer
- X Use common words or simple patterns
- X Ignore breach notifications

Password Strength Examples:

- password123 — Weak (Too common)
- Fluffy2019! — Weak (Personal info + pattern)
- X7k#mP2\$ — Medium (Good variety, but too short)
- correct-horse-battery — Medium (Long passphrase but lacking variety)
- Mango-42-Trumpet!sunset — Strong (Long passphrase with variety)
- adMf\$^78aBxfgGHJ!* — Very Strong (Long string of random characters with variety)

Notes & Action Items:

Need help with your password management?

Contact: ParksvilleTech.com • Support@ParksvilleTech.com • 1 (250) 228 6520

Serving the Oceanside Community & RDN with Professional Tech Support