Wigington Security Group

Privacy consulting for individuals and families

Password Manager Setup Guide

The single most important security tool you'll ever use

What You'll Learn:

- Why password managers are essential (not optional)
- Choosing the right password manager for your needs
- Step-by-step setup for 1Password, Bitwarden, and KeePassXC
- Migrating from browser-saved passwords
- Family sharing and emergency access
- Advanced features: passkeys, security keys, breach monitoring
- Best practices for long-term password hygiene

Time Investment:

- Initial setup: 1–2 hours
- Password migration: 3–5 hours over first week
- Ongoing: 5 minutes per month

This investment will save you hundreds of hours and prevent thousands in fraud losses.

February 2026 • 18 Pages • Free Download

wigingtonsecurity.com

Contents

1 Why You Need a Password Manager

1.1 The Password Problem

The average person has 100+ online accounts. Each requires a password. The human brain cannot:

- Remember 100+ unique, strong passwords
- Track which password goes with which account
- Remember when passwords were last changed
- Identify which passwords were exposed in breaches
- Generate cryptographically random passwords

So people do what's natural: they reuse passwords, use predictable patterns, or write them down insecurely.

Warning

The brutal statistics:

- 65% of people reuse passwords across multiple accounts
- 13% use the same password for ALL accounts
- Top password in 2024 breaches: "123456" (used millions of times)
- Average time to crack 8-character password: **39 seconds**
- 81% of data breaches involve weak or stolen passwords

1.2 What Happens Without a Password Manager

Real-world attack scenario:

1. LinkedIn gets breached (2021, 700 million accounts)
2. Your email and password are now public
3. Criminals use automated tools to try that password on:
   - Your bank
   - Gmail/Outlook
   - PayPal
   - Amazon
   - Every major service
4. If you reused that password, they're now in multiple accounts
5. They reset other passwords using your compromised email
6. Within hours: bank drained, identity stolen, credit ruined

This isn't hypothetical. This happens *thousands of times per day.*

1.3 What a Password Manager Does

A password manager is software that:

1. **Generates** cryptographically random passwords (20+ characters)
2. **Stores** passwords in encrypted database
3. **Auto-fills** passwords when you need them
4. **Syncs** across all your devices
5. **Alerts** you when passwords are reused or breached
6. **Organizes** your digital life in one secure place

You only remember one password: the master password to unlock your password manager.

CRITICAL

A password manager is not a convenience tool—it's a **security necessity**. It's the single most effective step you can take to protect yourself online.

If you do nothing else from this guide, **install and use a password manager**.

1.4 Common Objections (And Why They're Wrong)

1.4.1 "Isn't putting all my passwords in one place risky?"

No. Here's why:

- Your passwords are encrypted with military-grade encryption (AES-256)
- The password manager company cannot decrypt your passwords
- Even if the company's servers are breached, attackers get encrypted gibberish
- Your master password is the only decryption key
- This is far more secure than reusing passwords or writing them down

Real risk: Reusing "Password123" across 50 sites.
Lower risk: Using a password manager with a strong master password.

1.4.2 "I'll just write them down on paper"

Paper is actually better than password reuse, but has limitations:

- ✅ Can't be hacked remotely
- ❌ Can be lost, stolen, or destroyed (fire, flood)
- ❌ Doesn't work across devices
- ❌ No breach alerts
- ❌ Typing passwords manually is error-prone
- ❌ Doesn't help generate strong passwords

1.4.3 "My browser remembers my passwords"

Browser password managers are better than nothing, but have serious weaknesses:

Feature	Browser	Dedicated PM
Encryption	Varies, often weak	Strong (AES-256)
Cross-browser	No	Yes
Mobile apps	Limited	Full support
Security audits	Rare	Regular
Breach monitoring	Basic	Comprehensive
2FA/passkey support	Limited	Full
Secure notes	No	Yes
Emergency access	No	Yes
Password health report	Chrome only	All
Export	Plaintext (insecure)	Encrypted

Warning

Chrome's password manager stores passwords encrypted on Google's servers. If someone gets your Google password, they get ALL your passwords. A dedicated password manager uses zero-knowledge encryption—even the company can't access your passwords.

1.5 Who Needs a Password Manager

Everyone. But especially:

Checklist

- Anyone with online banking or financial accounts
- Anyone who has ever reused a password
- Parents managing family accounts
- Small business owners
- Anyone over age 13 with internet access
- People who have experienced account compromise
- Anyone who values their privacy and security

If you have more than 5 online accounts, you need a password manager. No exceptions.

2 Choosing the Right Password Manager

Not all password managers are equal. This section helps you choose based on your needs, technical comfort, and budget.

2.1 The Big Three Recommendations

We recommend three password managers based on extensive testing and security audits:

1. **1Password** — Best for most people
2. **Bitwarden** — Best for budget-conscious users
3. **KeePassXC** — Best for maximum control and privacy

Not recommended:

- LastPass (history of breaches, declining security)
- Dashlane (expensive, fewer features than competitors)
- Norton/McAfee password managers (inferior to dedicated tools)
- Any password manager without independent security audits

2.2 Detailed Comparison

Feature	1Password	Bitwarden	KeePassXC
Price	$2.99/mo individual, $4.99/mo family	Free, $10/yr premium	Free (open source)
Encryption	AES-256	AES-256	AES-256 or ChaCha20
Zero-knowledge	Yes	Yes	Yes (local only)
Open source	No	Yes	Yes
Cloud sync	Yes (built-in)	Yes (built-in)	Manual (Dropbox, etc.)
Browser extension	Excellent	Good	Good
Mobile apps	iOS, Android (excellent)	iOS, Android (good)	iOS, Android (basic)
Desktop apps	Mac, Windows, Linux	Mac, Windows, Linux	Mac, Windows, Linux
Security audits	Regular (Cure53)	Regular (multiple)	Community audited
2FA support	TOTP, security keys	TOTP (premium)	TOTP plugins
Passkey support	Yes	Yes	Limited
Breach monitoring	Watchtower (excellent)	Basic (premium)	None
Family sharing	Up to 5 members	Up to 6 (org)	Manual file sharing
Emergency access	Yes	Yes (premium)	Manual (file access)
Secure notes	Unlimited	Unlimited	Unlimited
File attachments	1GB documents	1GB (premium)	Any size (local)
Travel mode	Yes (hide vaults)	No	Manual (close app)
Customer support	Excellent	Email only	Community forums
Learning curve	Easy	Moderate	Advanced
Best for	Most users, families, ease of use	Budget users, tech-savvy	Privacy advocates, technical users

Feature	1Password	Bitwarden	KeePassXC
Jurisdiction	Canada	USA (but open source)	N/A (local)
Company model	Subscription revenue	Freemium + open source	Donation-supported
Master password	Required	Required	Required
Recovery options	Emergency kit, account recovery	None (you lose access)	Key file backup

Table 1: Comprehensive password manager comparison

2.3 Decision Framework

2.3.1 Choose 1Password if:

- You want the best user experience
- You're setting this up for family members (especially non-technical)
- You value excellent customer support
- Budget isn't a primary concern ($36–$60/year)
- You want travel mode and advanced features
- You need seamless sync across all devices
- You want regular security updates without thinking about it

1Password is our top recommendation for 90% of users.

2.3.2 Choose Bitwarden if:

- You want a free option that's still secure
- You prefer open-source software
- You're technically comfortable
- You want to self-host (advanced users)
- Budget is tight but security is important
- You don't need premium features like TOTP
- You're okay with slightly less polished interface

Bitwarden is the best free option, period.

2.3.3 Choose KeePassXC if:

- You want maximum privacy (no cloud sync)
- You're highly technical
- You don't trust any company with your data
- You want complete control over your database
- You're comfortable managing your own backups
- You can handle manual sync across devices
- You don't need mobile access (or can set up sync yourself)

KeePassXC is for privacy purists and technical users.

Pro Tip

Can't decide? Start with **1Password**. It has the easiest migration path if you change your mind later, and the user experience means you'll actually use it consistently.

The best password manager is the one you'll actually use. Don't let perfect be the enemy of good.

2.4 What About LastPass?

LastPass was once a top recommendation but is now **NOT recommended** due to:

- Multiple security breaches (2015, 2021, 2022)
- 2022 breach exposed customer vault data
- Poor incident response and communication
- Declining feature development
- Better alternatives available (1Password, Bitwarden)

Warning

If you currently use LastPass, migrate to 1Password or Bitwarden immediately. We'll cover migration in Section 4.

3 Step-by-Step Setup

This section provides detailed setup instructions for each recommended password manager.

3.1 1Password Setup

3.1.1 Step 1: Create Account

1. Visit https://1password.com
2. Click "Get Started"
3. Choose plan:
   - Individual: $2.99/month
   - Families: $4.99/month (up to 5 people) — **recommended for households**
4. Enter email address (use your secure email, not work email)
5. Create your account

3.1.2 Step 2: Create Your Master Password

This is the **most important password you'll ever create**.

CRITICAL

Master password requirements:

- Minimum 20 characters (longer is better)
- Mix of uppercase, lowercase, numbers, symbols
- NOT based on personal information
- NOT a password you've used anywhere else
- Something you can remember (you'll type it daily)
- NEVER write it down digitally

Recommended method: Diceware passphrase

1. Use 6–7 random words from Diceware list
2. Example: `correct-horse-battery-staple-mountain-river-cloud`
3. Modify with numbers/symbols: `Correct7Horse!Battery2Staple`
4. Easy to remember, extremely difficult to crack

Alternative: Sentence method

1. Think of a memorable sentence

2. Example: "My daughter Sarah was born in Seattle on March 15th 2018"
3. Take first letters: `MdSwbiSoM152018`
4. Add symbols: `Md5wb!SOM15$2018`

Warning

Write your master password on paper and store it in a secure physical location (safe, safety deposit box). This is the ONLY acceptable place to write it down.

If you forget your master password, your data is gone forever. 1Password cannot recover it.

3.1.3 Step 3: Download Emergency Kit

After creating your account, 1Password generates an Emergency Kit PDF:

1. Download the Emergency Kit
2. Print two copies
3. Fill in your master password on the printed copies (NOT the PDF)
4. Store copies in separate secure locations:
   - Copy 1: Home safe or locked drawer
   - Copy 2: Safety deposit box or trusted family member
5. Delete the PDF from your computer (it now contains your master password)

What's in the Emergency Kit:

- Your account email
- Your Secret Key (unique to your account)
- QR code for quick setup
- Space to write master password (do this on paper only)

3.1.4 Step 4: Install Apps

Desktop:

1. Download 1Password app for your OS (Mac/Windows/Linux)
2. Install and open
3. Sign in using Emergency Kit QR code or email + Secret Key + master password
4. Allow 1Password to integrate with system (enables auto-fill)

Browser Extension:

1. Visit https://1password.com/downloads/

2. Install extension for your browser (Chrome, Firefox, Safari, Edge)
3. Click 1Password icon in toolbar
4. Sign in (will connect to desktop app if installed)
5. Test auto-fill on a website

Mobile:

1. Download 1Password from App Store (iOS) or Google Play (Android)
2. Open app
3. Sign in using QR code from Emergency Kit (easiest) or manually
4. Set up biometric unlock (Face ID, Touch ID, fingerprint)
5. Enable AutoFill:
   - iOS: Settings → Passwords → AutoFill Passwords → 1Password
   - Android: Settings → System → Languages & input → Autofill service → 1Password

3.1.5 Step 5: Enable Two-Factor Authentication

Add 2FA to your 1Password account for extra protection:

1. Log into 1Password web interface: `https://my.1password.com`
2. Profile → Two-Factor Authentication
3. Choose method:
   - **Authenticator app:** Use separate app like Authy or 2FAS
   - **Security key:** Use YubiKey or similar hardware token (most secure)
4. Follow setup instructions
5. Save recovery codes in a secure location (print and store with Emergency Kit)

Pro Tip

Use a **separate** authenticator app for your 1Password 2FA codes. Don't store your 1Password 2FA code inside 1Password itself (that defeats the purpose).

Recommended: Install Authy or 2FAS on your phone specifically for 1Password 2FA.

3.2 Bitwarden Setup

3.2.1 Step 1: Create Account

1. Visit https://bitwarden.com
2. Click "Get Started"
3. Enter email address
4. Create master password (follow same guidelines as 1Password above)
5. Optional: Create password hint (don't make it too obvious)
6. Click "Submit"

3.2.2 Step 2: Verify Email

1. Check your email for verification link
2. Click link to verify account
3. You can now log in to Bitwarden

3.2.3 Step 3: Install Apps

Desktop:

1. Download Bitwarden desktop app from https://bitwarden.com/download/
2. Install for your OS (Windows, Mac, Linux)
3. Launch app
4. Log in with email and master password
5. Optional: Enable biometric unlock (fingerprint/Face ID)

Browser Extension:

1. Visit https://bitwarden.com/download/
2. Click your browser (Chrome, Firefox, Safari, Edge, etc.)
3. Install extension
4. Click Bitwarden icon in toolbar
5. Log in
6. Pin extension to toolbar for easy access

Mobile:

1. Download from App Store or Google Play
2. Install and open
3. Log in with email and master password
4. Enable biometric unlock
5. Set up AutoFill (same process as 1Password above)

3.2.4 Step 4: Enable Two-Factor Authentication

1. Log into web vault: https://vault.bitwarden.com
2. Settings → Two-step Login
3. Choose method:
   - Free: Authenticator app (recommended for most users)
   - Premium: FIDO2 WebAuthn (hardware security keys)
   - Premium: Duo, YubiKey OTP
4. For authenticator app:
   (a) Install separate 2FA app (Authy, 2FAS)
   (b) Scan QR code in Bitwarden
   (c) Enter code to verify
   (d) Save recovery code (print and store securely)

3.2.5 Step 5: Consider Premium (Optional)

Bitwarden free is excellent, but premium ($10/year) adds:

- TOTP code generation (built-in 2FA codes)
- 1GB encrypted file storage
- Hardware security key 2FA
- Priority customer support
- Vault health reports
- Emergency access

Our recommendation: Try free for a month, then upgrade to premium. $10/year is exceptional value.

3.3 KeePassXC Setup (Advanced)

⚠ Warning

KeePassXC is for technical users comfortable with manual setup and maintenance. If you're not sure, use 1Password or Bitwarden instead.

3.3.1 Step 1: Download and Install

1. Visit https://keepassxc.org/download/
2. Download for your OS (Windows, Mac, Linux)
3. Verify download signature (important for security):
   - Download signature file
   - Verify GPG signature matches official key
4. Install application

3.3.2 Step 2: Create New Database

1. Launch KeePassXC
2. Database → New Database
3. Choose location to save database file:
   - Recommended: Save in a folder you'll sync (Dropbox, Google Drive)
   - Name: `passwords.kdbx`
4. Configure database settings:
   - Encryption: AES-256 (default)
   - Key derivation: Argon2 (default, most secure)
5. Click "Continue"

3.3.3 Step 3: Set Master Password

1. Enter master password (same guidelines as above)
2. Re-enter to confirm
3. Optional: Add key file for additional security
   - Generate key file
   - Store in separate location from database
   - Backup key file (if you lose it, database is inaccessible)
4. Click "Done"

3.3.4 Step 4: Configure Browser Extension

1. Install KeePassXC-Browser extension:
   - Chrome: Chrome Web Store
   - Firefox: Firefox Add-ons
2. In KeePassXC: Tools → Settings → Browser Integration
3. Enable "Enable browser integration"
4. Check your browser(s)
5. Click extension icon in browser
6. Click "Connect" to link extension with KeePassXC
7. Test on a website

3.3.5 Step 5: Set Up Sync (Manual)

KeePassXC doesn't have built-in sync. Options:

Option 1: Cloud Storage Sync

1. Save database file in Dropbox/Google Drive/OneDrive folder
2. Access from multiple devices via cloud folder
3. **Pros:** Simple, automatic sync
4. **Cons:** Database file in cloud (but encrypted)

Option 2: Syncthing (Privacy-Focused)

1. Install Syncthing on all devices
2. Configure peer-to-peer sync
3. Database syncs directly between your devices
4. **Pros:** No cloud storage, completely private
5. **Cons:** More complex setup

Option 3: Manual Copy

1. Manually copy database file to each device
2. Remember to sync regularly
3. **Pros:** Maximum control
4. **Cons:** Easy to forget, can create conflicts

3.3.6 Step 6: Mobile Setup

iOS: KeePassium or Strongbox

1. Download KeePassium from App Store
2. Open database from Files app (if using iCloud)
3. Or add from Dropbox/Google Drive
4. Enter master password (and key file if using)
5. Enable Face ID/Touch ID

Android: KeePassDX

1. Download KeePassDX from Google Play
2. Open database from storage
3. Enter master password
4. Enable fingerprint unlock

Pro Tip

KeePassXC backup strategy:
Since you're managing your own database file:

1. Set up automatic backups of database file
2. Keep backup in separate location from primary
3. Test restoring from backup quarterly
4. Keep old versions in case of corruption

Your database file is your entire password vault. Treat it like gold.

4 Migrating Your Passwords

You have passwords scattered across browsers, sticky notes, and memory. Time to consolidate them securely.

4.1 Where Are Your Passwords Now?

4.1.1 Browser-Saved Passwords

Most people have passwords saved in:

- Chrome password manager
- Firefox Lockwise
- Safari Keychain
- Edge password manager

We'll export these and import into your password manager.

4.1.2 Written Passwords

- Sticky notes on monitor
- Notebook in drawer
- Text file on desktop
- Spreadsheet

We'll manually add these, then securely destroy originals.

4.1.3 Memory

Important passwords you "just know" but nowhere else.
We'll add these and generate strong replacements.

4.2 Exporting from Chrome

1. Open Chrome
2. Settings → Autofill → Passwords
3. Click three dots next to "Saved Passwords"
4. Select "Export passwords"
5. Authenticate with your computer password
6. Save CSV file to Desktop (temporary)
7. File contains passwords in **plain text**—very sensitive

CRITICAL

The exported CSV contains all your passwords unencrypted. Treat it like gold:

- Don't email it to yourself
- Don't save it in cloud storage
- Delete it immediately after importing
- Empty trash after deleting

4.3 Importing to 1Password

1. Open 1Password desktop app
2. File → Import
3. Select "Chrome" as source
4. Choose the CSV file you exported
5. Click "Import"
6. Review imported passwords (1Password shows summary)
7. Imported passwords appear in your vault

After import:

1. Verify passwords imported correctly (spot check 5–10)
2. Delete CSV file from Desktop
3. Empty Trash
4. In Chrome: Settings → Passwords → Turn off "Offer to save passwords"
5. Don't delete Chrome passwords yet (wait 2 weeks to confirm everything works)

4.4 Importing to Bitwarden

1. Open web vault: `https://vault.bitwarden.com`
2. Tools → Import Data
3. Select format: "Chrome (csv)"
4. Click "Choose File" and select exported CSV
5. Click "Import Data"
6. Review import results

After import:

1. Check that passwords imported correctly
2. Delete CSV file
3. Empty Trash
4. Disable Chrome password saving

4.5 Importing to KeePassXC

1. Open KeePassXC
2. Database → Import → CSV File
3. Select Chrome CSV export
4. Map columns:
   - Column 1: Title/Name
   - Column 2: Username
   - Column 3: Password
   - Column 4: URL
5. Click "OK" to import
6. Review entries in database

4.6 Exporting from Other Browsers

4.6.1 Firefox

1. about:logins in address bar
2. Three dots menu → Export Logins
3. Save CSV file
4. Import using same process as Chrome above

4.6.2 Safari (macOS)

Safari doesn't have direct export, but:

Method 1: Manual copy

1. System Preferences → Passwords
2. Authenticate
3. Manually copy passwords to your password manager

Method 2: Use 1Password extension

1. Install 1Password Safari extension
2. When you visit a site, 1Password offers to save Safari's saved password
3. Accept for each site
4. Slower but works

4.6.3 Edge

1. Settings → Profiles → Passwords
2. Three dots → Export passwords
3. Save CSV
4. Import to password manager

4.7 Manually Adding Passwords

For passwords not in browsers (written down, in memory):

4.7.1 In 1Password

1. Click "+" (New Item)
2. Choose type: Login
3. Fill in:
   - Title: Website or service name
   - Username: Your username/email
   - Password: Current password
   - Website: Full URL
4. Add to appropriate vault
5. Click "Save"

4.7.2 In Bitwarden

1. Click "+" (Add Item)
2. Select "Login"
3. Fill in Name, Username, Password, URL
4. Save

4.7.3 In KeePassXC

1. Entries → Add New Entry
2. Title: Service name
3. Username: Your username
4. Password: Current password
5. URL: Website
6. Click OK

4.8 Testing Your Setup

Before deleting old passwords:

Checklist

- [ ] Test auto-fill on 5–10 different websites
- [ ] Test on mobile device
- [ ] Verify passwords in different categories (banking, email, shopping)
- [ ] Confirm browser extension works correctly
- [ ] Test generating and saving a new password
- [ ] Use password manager for one week before deleting old sources

4.9 Cleaning Up Old Password Storage

After 2 weeks of successful use:

1. **Browser passwords:**
   - Chrome: Settings → Passwords → Delete all saved passwords
   - Firefox: about:logins → Remove all
   - Keep "Offer to save" disabled
2. **Written passwords:**
   - Shred sticky notes
   - Destroy notebooks
   - Delete text files
   - Securely wipe spreadsheets
3. **Verify nothing left behind:**
   - Search computer for "passwords.txt", "logins.doc", etc.
   - Check desk drawers
   - Check phone notes app

5 Password Manager Best Practices

Having a password manager is step one. Using it correctly is step two.

5.1 Generating Strong Passwords

5.1.1 Using Built-in Password Generator

1Password:

1. When creating/editing login, click password field
2. Click generator icon
3. Adjust settings:
   - Length: 20+ characters recommended
   - Include symbols, numbers
   - Random (not memorable) for maximum security
4. Click "Fill" to use generated password

Bitwarden:

1. Click generator icon (top right)
2. Select Password type
3. Set length: 18+ characters
4. Enable all character types
5. Click "Copy" or "Select"

KeePassXC:

1. Right-click password field
2. Generate Password
3. Configure length and character sets
4. Click OK

5.1.2 Password Generation Rules

- **Minimum 16 characters** (20+ preferred)
- **Use all character types:** uppercase, lowercase, numbers, symbols
- **Random is better than memorable** (password manager remembers for you)
- **Unique for every account** (never reuse)
- **Don't use patterns** ("Password1", "Password2" are not unique)

Pro Tip

When to use memorable passwords:
Only for passwords you'll type frequently without auto-fill:

- Master password
- Computer login
- Phone unlock (though biometrics preferred)

Everything else: maximum random length.

5.2 Organizing Your Vault

5.2.1 Using Categories/Folders

Organize passwords for easy finding:

Recommended folder structure:

- Banking & Finance
- Email & Cloud
- Shopping & Retail
- Social Media
- Work Accounts
- Subscriptions & Memberships
- Utilities & Services
- Family Accounts (shared vault)

5.2.2 Using Tags (1Password/Bitwarden)

Add tags for cross-category organization:

- `high-security` — Financial, email, critical accounts
- `2fa-enabled` — Accounts with 2FA
- `shared` — Shared with family
- `needs-update` — Passwords to change
- `rarely-used` — Accounts accessed infrequently

5.2.3 Adding Notes and Context

Use the Notes field for:

- Security questions and answers
- Account numbers
- Customer service phone numbers
- Recovery codes
- Special instructions
- Account setup date

Example note:

```
Account created: 2023-01-15
Security questions:
- Mother's maiden name: PurpleElephant92 (fake answer)
- First pet: BlueMountain77 (fake answer)
Recovery email: backup@protonmail.com
Last password change: 2024-02-10
Notes: This account requires phone 2FA. Keep phone nearby.
```

5.3 Enabling Breach Monitoring

Password managers can alert you to compromised passwords.

5.3.1 1Password Watchtower

1. Automatically enabled
2. Monitors for:
    - Passwords exposed in breaches
    - Reused passwords
    - Weak passwords
    - Unsecured websites (HTTP)
    - Inactive 2FA
    - Expiring items
3. View alerts: Watchtower section in app
4. Act on warnings immediately

5.3.2 Bitwarden Vault Health Reports

1. Premium feature (free in organizations)
2. Reports → Vault Health
3. Shows:
   - Exposed passwords (Have I Been Pwned)
   - Reused passwords
   - Weak passwords
4. Fix issues one by one

5.3.3 Manual Breach Checking

1. Visit https://haveibeenpwned.com
2. Enter email addresses
3. Check which services breached
4. Change those passwords immediately
5. Enable HIBP monitoring in password manager

5.4 Regular Password Hygiene

5.4.1 Monthly Tasks

☑ Checklist

- ☐ Check Watchtower/Health Reports for alerts
- ☐ Update any flagged passwords
- ☐ Remove passwords for deleted accounts
- ☐ Review shared passwords (family vault)

5.4.2 Quarterly Tasks

☑ Checklist

- ☐ Change passwords for high-value accounts (bank, email)
- ☐ Review and update security questions
- ☐ Check 2FA status on critical accounts
- ☐ Update recovery information
- ☐ Review shared access permissions

5.4.3 Annual Tasks

Checklist

- [ ] Change master password
- [ ] Review all passwords for patterns
- [ ] Delete unused account logins
- [ ] Update Emergency Kit
- [ ] Test emergency access procedures
- [ ] Review subscription (renew premium if needed)

6 Family Sharing and Emergency Access

6.1 Setting Up Family Sharing

6.1.1 1Password Families

1. Sign up for 1Password Families ($4.99/month, up to 5 people)
2. Invite family members:
   - Send invitation via email
   - They create their own account and master password
   - They get access to shared vault
   - Each person has private vault too
3. Create shared vaults:
   - "Family Shared" — passwords everyone needs (Netflix, utilities)
   - "Parents Only" — financial accounts
   - "Kids Shared" — age-appropriate passwords

What to share:

- Streaming services (Netflix, Disney+)
- Utilities and home services
- Wifi passwords
- Shared shopping accounts
- Family memberships

What NOT to share:

- Personal email passwords
- Individual bank accounts
- Personal social media
- Work accounts
- Anything privacy-sensitive

6.1.2 Bitwarden Organizations

1. Create free organization (up to 2 users) or Families plan ($1/month/user)
2. Invite family members
3. Create collections:
   - Shared Streaming
   - Home Services
   - Family Accounts
4. Assign permissions per person

6.2 Emergency Access

What happens if you're incapacitated? Your family needs access to critical accounts.

6.2.1 1Password Emergency Access

Not available yet in 1Password, but planned. Current workaround:

1. Store Emergency Kit in accessible location
2. Designate trusted person
3. Give them location of Emergency Kit (but not the kit itself)
4. Include master password in will or with lawyer

6.2.2 Bitwarden Emergency Access (Premium)

1. Settings → Emergency Access
2. Add trusted emergency contact (email required)
3. They accept invitation
4. Set wait time (0–90 days)
    - 0 days: immediate access (use carefully)
    - 30 days: balance of security and urgency
    - 90 days: maximum security
5. If you become unavailable:
    - Emergency contact requests access
    - You have wait period to reject
    - If no rejection, they get view or takeover access

6.3 Teaching Family Members

6.3.1 For Non-Technical Users

1. **Start simple:**
    - Install app on their devices
    - Show them how to auto-fill on 2–3 sites
    - Let them use it for a week
2. **Gradually expand:**
    - Add more passwords
    - Teach password generation
    - Show secure notes feature

3. **Emphasize master password importance:**
    - Must be memorable
    - Must be written down (physically)
    - Cannot be recovered if forgotten

6.3.2 For Children/Teens

- Create family vault with age-appropriate access
- Teach password hygiene early
- Monitor their use initially
- Gradually give more independence
- Use it as teaching opportunity about online security

Pro Tip

Getting family buy-in:
Frame it as convenience, not just security:

- "Never forget passwords again"
- "Log in with one click"
- "Share Netflix password easily"
- "Works on phone and computer"

Security benefits come naturally once they're using it.

7 Advanced Features

7.1 TOTP Two-Factor Codes

Password managers can generate 2FA codes (like Google Authenticator).

7.1.1 When to Use This Feature

Arguments FOR storing 2FA in password manager:

- Convenience: one app for passwords and 2FA
- Never lose access if you lose phone
- Works across all devices
- Better than no 2FA at all

Arguments AGAINST:

- Reduces 2FA to "something you have" only (not two factors)
- If password manager compromised, attacker gets both
- Defeats purpose of two-factor authentication

Our recommendation:

- **High-security accounts** (bank, email, password manager itself): Use separate 2FA app or hardware key
- **Medium-security accounts** (social media, shopping): OK to store in password manager
- **Low-security accounts** (forums, newsletters): Definitely store in password manager

7.1.2 Setting Up TOTP in 1Password

1. Edit login item
2. Click "One-Time Password"
3. When setting up 2FA on website:
    - Instead of scanning with phone, click "Can't scan?"
    - Copy secret key
    - Paste into 1Password
4. 1Password now generates codes
5. When logging in, 1Password auto-fills code

7.1.3 Setting Up TOTP in Bitwarden

1. Premium feature
2. Edit item → Authenticator Key (TOTP)
3. Scan QR code or enter secret key
4. Bitwarden generates 6-digit codes
5. Codes auto-fill when needed

7.2 Passkeys (FIDO2/WebAuthn)

Passkeys are the future of authentication—stronger than passwords.

7.2.1 What Are Passkeys?

- Cryptographic keys stored in password manager
- Phishing-resistant (tied to specific website)
- No password needed (biometric or PIN)
- Supported by Apple, Google, Microsoft
- Growing site adoption (PayPal, Best Buy, GitHub, etc.)

7.2.2 Using Passkeys in Password Managers

1Password:

- Automatically saves passkeys when sites offer them
- Auto-fills using biometric (Face ID, fingerprint)
- Syncs across devices
- Gradually replace passwords with passkeys

Bitwarden:

- Passkey support in development
- Check latest updates for availability

When offered passkey option, use it. It's more secure than passwords.

7.3 Secure Notes and Documents

Password managers store more than just passwords.

7.3.1 What to Store

- **Secure notes:**
  - Wifi passwords
  - Security question answers
  - Software license keys
  - Important account numbers
  - Backup codes
  - Combinations (safe, locks)
- **Documents:**
  - Passport scans
  - Insurance cards
  - Medical records
  - Tax documents
  - Legal documents

7.3.2 Document Storage Limits

- **1Password:** 1GB total (Families plan)
- **Bitwarden:** 1GB (Premium)
- **KeePassXC:** Unlimited (local storage)

7.4 Travel Mode (1Password)

Temporarily hide sensitive vaults when crossing borders.

7.4.1 How It Works

1. Before travel: Enable Travel Mode at https://my.1password.com
2. Mark vaults as "Safe for Travel"
3. Other vaults become hidden on all devices
4. Cross border with only travel-safe passwords
5. After arrival: Disable Travel Mode
6. All vaults reappear

Use case: Prevent border agents from compelling access to sensitive accounts during device searches.

8 Final Checklist and Next Steps

8.1 Setup Completion Checklist

8.2 Ongoing Maintenance Schedule

Weekly:

- Use password manager for all new accounts
- Update existing passwords as you use them

Monthly:

- Check security alerts (Watchtower/Health Reports)
- Change flagged passwords
- Remove deleted accounts

Quarterly:

- Change passwords for financial accounts
- Review 2FA status
- Update security questions
- Check shared vault access

Annually:

- Change master password
- Update Emergency Kit
- Test recovery procedures
- Review subscription/features
- Delete unused accounts

8.3 What's Next

Now that you have a password manager:

1. **Enable 2FA everywhere:** Use our guide *Email Security & Privacy*
2. **Clean up data brokers:** Use our guide *Complete Data Broker Removal*
3. **Harden your devices:** Use our guide *Phone & Device Hardening*
4. **Lock down social media:** Use our guide *Social Media Privacy Configuration*
5. **Plan for the worst:** Use our guide *Digital Estate Planning*

8.4 Additional Resources

Password Manager Documentation:

- 1Password: https://support.1password.com
- Bitwarden: https://bitwarden.com/help/
- KeePassXC: https://keepassxc.org/docs/

Breach Monitoring:

- Have I Been Pwned: https://haveibeenpwned.com
- WigSec Breach Checker: https://wigingtonsecurity.com/tools/breach-check

Password Security Tools:

- Password strength tester: https://www.passwordmonster.com
- Diceware generator: https://diceware.dmuth.org

☑ Checklist

Need Help With Password Manager Setup?

We offer personalized setup assistance and security audits.
Contact: https://wigingtonsecurity.com/contact
Services: https://wigingtonsecurity.com/services

One-on-one consultations available for families and small businesses

Document Version 1.0 • February 2026

https://wigingtonsecurity.com